EBA/GL/2019/02

25 February 2019

Final Report on

EBA Guidelines on outsourcing arrangements

Contents

Executive summary

Trust in the reliability of the financial system is crucial for its proper functioning and is a prerequisite if it is to contribute to the economy as a whole. Effective internal governance arrangements are fundamental if institutions individually and the financial system they form as a whole are to operate well.

Over recent years, financial institutions have been increasingly interested in outsourcing business activities also in order to reduce costs and improve their flexibility and efficiency. In the context of digitalisation and the increasing importance of new financial technology (fintech) providers, financial institutions are adapting their business models to embrace such technologies. Some have intensified the use of fintech solutions and have launched projects to improve their cost efficiency also in response to the intermediation margins of the traditional banking business model being put under pressure by the low interest rate environment. Outsourcing is a way to get relatively easy access to new technologies and to achieve economies of scale.

Directive 2013/36/EU (Capital Requirements Directive; CRD) strengthens the governance requirements for institutions and Article 74(3) CRD gives the EBA the mandate to develop guidelines on institutions' governance arrangements. Outsourcing is one of the specific aspects of institutions' governance arrangements. Directive 2014/65/EU (Markets in Financial Instruments Directive; MiFID II) contains explicit provisions regarding the outsourcing of functions in the field of investment services and activities. Directive 2015/2366/EU (Revised Payment Service Directive; PSD2) sets out requirements for the outsourcing of functions by payment institutions.

The EBA is updating the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing that were issued in 2006, which applied exclusively to credit institutions; the aim is to establish a more harmonised framework for all financial institutions that are within the scope of the EBA's mandate, namely credit institutions and investment firms subject to the CRD, as well as payment and electronic money institutions. The guidelines set out specific provisions for these financial institutions' governance frameworks with regard to their outsourcing arrangements and the related supervisory expectations and processes. The recommendation on outsourcing to cloud service providers, published in December 2017, has been integrated into the guidelines.

Each financial institution's management body remains responsible for that institution and all of its activities, at all times; to this end, the management body should ensure that sufficient resources are available to appropriately support and ensure the performance of those responsibilities, including overseeing all risks and managing the outsourcing arrangements. Outsourcing must not lead to a situation in which an institution becomes an 'empty shell' that lacks the substance to remain authorised.

With regard to outsourcing to service providers located in third countries, financial institutions are expected to take particular care that compliance with EU legislation and regulatory requirements

(e.g. professional secrecy, access to information and data, protection of personal data) is ensured and that the competent authority is able to effectively supervise financial institutions, in particular regarding critical or important functions outsourced to service providers.

The guidelines set out which arrangements with third parties are to be considered as outsourcing and provide criteria for the identification of critical or important functions that have a strong impact on the financial institution's risk profile or on its internal control framework. If such critical or important functions are outsourced, stricter requirements apply to these outsourcing arrangements than to other outsourcing arrangements.

Competent authorities are required to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring risk concentrations at individual service providers and assessing whether or not such concentrations could pose a risk to the stability of the financial system. To identify such risk concentrations, competent authorities should be able to rely on comprehensive documentation on outsourcing arrangements compiled by financial institutions.

Next steps

The guidelines will enter into force on 30 September 2019. The 2006 guidelines on outsourcing and the EBA's recommendation on outsourcing to cloud service providers will be repealed at the same time.

Background

1. Trust in the reliability of the financial system is crucial for its proper functioning and is a prerequisite if it is to contribute to the economy as a whole. Effective internal governance arrangements are fundamental if credit institutions and investment firms subject to Directive 2013/36/EU[1] (CRD) (both referred to as 'institutions'), payment institutions and electronic money institutions (both referred to as 'payment institutions') and the financial system they form part of are to operate well.

2. Over recent years, there has been an increasing tendency by institutions and payment institutions to outsource activities also in order to reduce costs and improve flexibility and efficiency. In the context of digitalisation and the increasing importance of information technology (IT) and financial technologies (fintech), institutions and payment institutions are adapting their business models, processes and systems to embrace such technologies. IT has become one of the most commonly outsourced activities. Notwithstanding its benefits, outsourcing IT and data services poses security issues and challenges to the governance framework of institutions and payment institutions, in particular to internal controls as well as to data management and data protection.

3. Some institutions and payment institutions have intensified the use of IT and fintech solutions and have launched projects to improve their cost efficiency also in response to the intermediation margins of the traditional banking lending model being put under pressure by the low interest rate environment. Outsourcing is a way to get relatively easy access to new technologies and to achieve economies of scale, e.g. by centralising functions within a group or institutional protection scheme.

4. The importance of outsourcing functions to cloud service providers has increased rapidly in many industries. In 2017, the EBA addressed the specificities of outsourcing to the cloud by developing recommendations on outsourcing to cloud service providers,[2] which were based on the 2006 CEBS outsourcing guidelines. The recommendations aimed at overcoming the high level of uncertainty regarding supervisory expectations on outsourcing to cloud service providers and at removing the barriers that this uncertainty caused for institutions proceeding with using cloud services. The recommendations have been integrated in the present guidelines and will be repealed when the guidelines enter into force.

5. Outsourcing of important or critical functions, in particular when the service provider is located outside the EU, creates specific risks both for institutions and payment institutions and for their competent authorities and should be subject to appropriate oversight. Any outsourcing that

[1] 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.

[2] The recommendation is available on the EBA's website under the following link: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers

would result in the delegation by the management body of its responsibility, altering the relationship and obligations of the institution or payment institution towards its clients, undermining the conditions of its authorisation or removing or modifying any of the conditions subject to which the institution's or payment institution's authorisation was granted, should not be permitted. Outsourcing arrangements should not create undue operational risks or impair the quality and independence of institutions' and payment institutions' internal controls or the ability of those institutions and payment institutions and the competent authorities to oversee and supervise compliance with regulatory requirements.

6. The responsibility of the institutions' and payment institutions' management body for the institution or payment institution and all its activities can never be outsourced.

7. Outsourcing is also relevant in the context of gaining or maintaining access to the EU's financial market. Third-country institutions and payment institutions may wish to set up subsidiaries or branches in the EU to get or maintain access to the EU's financial markets and infrastructures. In this context, third-country institutions and payment institutions may seek to minimise the transfer of the effective performance of business activities to their subsidiaries and branches located in the EU, e.g. by relying on the outsourcing of functions to the third-country parent institution or other third-country group entities.

8. Outsourcing must not lead to a situation where an institution or a payment institution 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 outsourcing arrangements.

9. Functions that are considered critical under a resolution perspective may also be outsourced. Outsourcing arrangements should not create impediments to the resolvability of the institution.

10. Competent authorities must grant authorisation in full compliance with Union law; should set a strict framework, in line with these guidelines, on outsourcing by institutions and payment institutions in the EU to third-country entities; and should ensure consistent and effective supervision. Competent authorities should also ensure that institutions and payment institutions have policies and procedures in place to comply with the relevant framework at all times.

11. Institutions and payment institutions should be able to effectively control and challenge the quality and performance of outsourced functions and be able to carry out their own risk assessment and ongoing monitoring. It is not sufficient for institutions and payment institutions to undertake only formal assessments of whether or not outsourced functions meet regulatory requirements.

12. The guidelines should be read in conjunction with, but without prejudice to, the EBA Guidelines on internal governance (which already include requirements on institutions' outsourcing policies), the EBA Guidelines on common procedures and methodologies for the supervisory

review and evaluation process (SREP) and the EBA Guidelines on information and communication technology (ICT) risk assessment under the SREP.

13. For payment institutions, these guidelines should be read in conjunction with the EBA Guidelines on the information to be provided for the authorisation of payment institutions under Directive 2015/2366/EU[3] (PSD2), the EBA Guidelines on security measures for operational and security risks under the PSD2[4] and EBA Guidelines on major incident reporting under the PSD2.[5]

14. All requirements set out in these guidelines are subject to the principle of proportionality; they are to be applied in a manner that is appropriate, taking into account, in particular, the institution's or payment institution's size and internal organisation and the nature, scope and complexity of its activities.

Rationale and objective of the guidelines

15. The EBA is updating the CEBS guidelines on outsourcing issued in 2006, which applied exclusively to credit institutions, with the aim of establishing a more harmonised framework for the outsourcing arrangements of financial institutions. The scope of application of these guidelines covers not only credit institutions and investment firms subject to the CRD (referred to as 'institutions'), but also payment and electronic money institutions (referred to as 'payment institutions'). The guidelines are not directly addressed to credit intermediaries and non-bank creditors that are subject to Directive 2014/17/EU[6] or to account information service providers that are only registered for the provision of service 8 of Annex I to the PSD2. Outsourcing arrangements between institutions, payment institutions and such entities are within the scope of the guidelines when such entities act as outsourcing service providers.

16. The update of the guidelines takes into account and is consistent with the current requirements under the CRD, Directive 2014/65/EU[7] (MiFID II), Directive 2009/110/EC[8] (Electronic Money Directive; EMD), the PSD2 and Directive 2014/59/EU[9] (Bank Recovery and Resolution Directive;

[3] 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.

[4] https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[5] https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

[6] 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.

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

[8] 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.

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

BRRD) and the respective delegated regulations adopted by the European Commission. In addition, international developments in this area, such as the revised corporate governance principles for banks and the guidelines on step-in risk published by the Basel Committee on Banking Supervision (BCBS), have been taken into account.

17. Under Article 16 of Regulation (EU) No 1093/2010[10] (the EBA Regulation), the EBA is required to issue guidelines and recommendations addressed to competent authorities and financial institutions with a view to establishing consistent, efficient and effective supervisory practices and ensuring the common, uniform and consistent application of Union law. In particular, the conditions for outsourcing of functions of banking activities by institutions are not harmonised to the same extent as for institutions and payment institutions subject to MiFID II and PSD2.

18. 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 outsourcing of functions by institutions and payment institutions to third countries, where supervisory authorities may lack the necessary powers and tools to adequately and effectively supervise service providers that provide critical or important functions to EU institutions and payment institutions.

19. It is necessary to provide a clear definition of what is considered outsourcing. The definition provided in the guidelines is in line with the related Commission Delegated Regulation (EU) 2017/565[11] supplementing MiFID II.

20. The use of the term 'critical or important functions' is based on the wording of MiFID II and the Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II. It is used only for the purpose of identifying 'critical or important functions' under outsourcing arrangements to which a specific set of requirements apply. Commission Delegated Regulation (EU) 2017/565 specifies, under Article 30, that 'an operational function shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities'. The same approach exists under Directive 2009/138/EC[12] (Solvency II), while, in the context of outsourcing, the PSD2 uses 'important function' for the purpose of identifying functions under outsourcing arrangements for which specific requirements apply. Therefore, to embrace all existing legislation and to ensure a level playing field for credit institutions, investment firms, payment institutions and electronic money institutions, the wording used under MiFID II is used within the guidelines. It should be noted

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

[11] 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.

[12] 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

that the definition of 'critical or important function' for the purpose of outsourcing used in these guidelines is different from the definition of 'critical functions' under Article 2(1)(35) BRRD.

21. Article 109(2) CRD requires that parent undertakings and subsidiaries subject to this Directive meet the governance requirements not only on a solo basis but also on a consolidated or sub-consolidated basis, unless waivers for the application on a solo basis have been granted under Article 21 CRD or Article 109(1) CRD in conjunction with Article 7 of Regulation (EU) No 575/2013 (Capital Requirements Regulation; CRR).[13] 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, as well as firms subject to Directive 2011/61/EU[14] and Directive 2009/65/EC[15]). Governance arrangements, processes and mechanisms must be consistent and well integrated and those subsidiaries not subject to the CRD must also be able to produce any data and information relevant for the purpose of supervision.

Governance of outsourcing arrangements

22. In accordance with Article 74 CRD, institutions and payment institutions (in line with Article 11 PSD2) should have robust internal governance arrangements that include a clear organisational structure. Outsourcing arrangements are one aspect of institutions' and payment institutions' organisational structure. The guidelines include requirements that aim to ensure that:

    a. there is effective day-to-day management by senior management or the management body;[16]

    b. there is effective oversight by the management body;

    c. there is a sound outsourcing policy and there are sound outsourcing processes;

    d. institutions and payment institutions have an effective and efficient internal control framework, including with regard to their outsourced functions;

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

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

[14] 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

[15] 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)

[16] Payment institutions should refer to the definition of a 'management body' and 'senior management' under the guidelines on the security measures for operational and security risks of payment services under PSD2 published in December 2017 on the EBA's website: https://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-security-measures-under-psd2

f. there are appropriate plans for the exit from outsourcing arrangements of critical or important functions, e.g. by migrating to another service provider or by reintegrating the critical or important outsourced functions; and

g. competent authorities remain able to effectively supervise institutions and payment institutions, including the functions that have been outsourced.

23. Institutions and payment institutions must determine whether the function to be outsourced is considered critical or important. The guidelines provide criteria to ensure that the assessment of the criticality or importance of functions is more harmonised. Outsourcing of critical and important functions can have a strong impact on the institution's or payment institution's risk profile. To this end, additional requirements apply to the outsourcing of critical or important functions, which aim to ensure the soundness of their governance arrangements and that competent authorities can exercise effective supervision.

24. While the guidelines focus on the outsourcing of critical or important functions, institutions and payment institutions need to consider that receiving services, including IT services, from third parties creates risks, even when those arrangements are not considered to be outsourcing arrangements or when the outsourcing arrangements would concern functions that are not critical or important. To manage all risks, institutions and payment institutions should assess the risks that result or may result from those arrangements, in particular the operational and reputational risk.

25. The risks to be considered include those associated with the institution's or the payment institution's relationship with the service provider, the risk caused by allowing for sub-outsourcing, the concentration risk posed by multiple outsourcings to the same service provider and/or the concentration risk posed by outsourcing critical or important functions to a limited number of service providers. The concentration of outsourcing at a limited number of service providers is particularly relevant for competent authorities when supervising the impact of outsourcing on the stability of the financial market. In addition, overreliance on outsourcing of 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.

26. Similarly, outsourcing arrangements with long or complex operational chains and/or with a large number of parties involved are likely to result in additional challenges both for institutions and payment institutions and for competent authorities.

27. Each form of outsourcing has its specific risks and advantages. Without prejudice to the waivers included in Articles 21 CRD that may be granted when the conditions under Article 10 of CRR are met and waivers under Article 109(1) CRD that apply when the derogation under Article 7 CRR has been granted by competent authorities, intragroup outsourcing is subject to the same regulatory framework as outsourcing to service providers outside the group. Intragroup outsourcing is not necessarily less risky than outsourcing to an entity outside the group. In particular, with regard to intragroup outsourcing, institutions and payment institutions need to

take into account conflicts of interest that may be caused by outsourcing arrangements, e.g. between different entities within the scope of consolidation.

28. Where institutions and payment institutions intend to outsource important or critical functions to entities within the same group, they should ensure that the selection of a group entity is based on objective reasons and that the conditions of the outsourcing arrangement are set at arm's length and explicitly deal with conflicts of interest that such an outsourcing arrangement may entail. Institutions and payment institutions should clearly identify all relevant risks and detail the mitigation measures and controls put in place to ensure that the outsourcing arrangements with affiliated entities do not impair the institution's or payment institution's ability to comply with the relevant regulatory framework. However, when outsourcing within the same group, institutions and payment institutions may have a higher level of control over the outsourced function, which they could take into account in their risk assessment.

29. The same aspects that are relevant for outsourcing within a group hold true when institutions that are members of an institutional protection scheme outsource functions to a central service provider.

30. Outsourcing critical or important functions to service providers located in third countries must be subject to additional safeguards that ensure that this outsourcing does not lead to an undue increase in risk or does not impair the ability of competent authorities to effectively supervise institutions and payment institutions.

31. Institutions must also have robust governance arrangements in place for outsourcing arrangements that are not considered critical or important. Therefore, the guidelines provide some requirements that apply to all outsourcing arrangements and more generally to all arrangements with third parties, taking into account the application of the proportionality principle.

32. Outsourcing does not lower institutions' and payment institutions' obligation to comply with regulatory requirements and internal corporate values, e.g. those set out within a code of conduct. When selecting service providers, institutions and payment institutions should carefully pay attention to human rights and take into account the impact of their outsourcing on all stakeholders; this includes taking into account their social and environmental responsibilities. Such aspects are of particular relevance when service providers are located in third countries.

33. Institutions and payment institutions need to manage the contractual relationship; this includes evaluating and monitoring the ability of the service provider to fulfil the conditions included in the written outsourcing agreement. Indeed, increased reliance on the service provider regarding the outsourced functions, in particular with regard to critical or important functions, may have an impact on institutions' and payment institutions' ability to manage their risks, such as operational risks, including compliance and reputational risks.

34. Specific guidance is provided on the relationship between institutions, payment institutions and service providers, including on their rights and obligations. The guidelines specify a set of aspects that should be included within the written outsourcing agreement.

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

36. The institutions', payment institutions' and competent authorities', including resolution authorities, right to inspections and access to information, accounts and premises should be ensured within the written outsourcing agreement. The right to audit is key to providing the appropriate assurance that at least critical or important outsourced functions, as well as functions that may become critical or important in the future, are provided as contractually agreed and in line with regulatory requirements. However, audit and access rights for competent authorities need to be ensured for all outsourcing arrangements to ensure that institutions can be effectively supervised. Further guidance is provided on how institutions and payment institutions can exercise their audit rights in a risk-based manner, taking into account concerns regarding the organisational burden for both the outsourcing institution or payment institution and the service provider, as well as practical, security and confidentiality concerns regarding physical access to certain types of business premises and access to data in multi-tenant environments.

IT outsourcing, including fintech and outsourcing to cloud service providers

37. Institutions and payment institutions must ensure that personal data are adequately protected and kept confidential. Institutions and payment institutions fall within the scope of application of Regulation (EU) 2016/679[17] (General Data Protection Regulation; GDPR) and must comply with it. When outsourcing IT or data services, it is imperative that business continuity and data protection are appropriately considered. Such considerations are not limited to the outsourcing of IT but apply in general. Institutions and payment institutions must ensure that they meet internationally accepted information security standards and this also applies to outsourced IT infrastructures and services.

38. Institutions and payment institutions need to have business continuity and contingency arrangements in place to ensure that their material business activities can be performed on a continuous basis. Therefore, such arrangements are also required from some service providers, in particular regarding outsourced functions that are critical or important.[18]

39. The EBA identified differences in national regulatory and supervisory frameworks for cloud outsourcing, e.g. with regard to the information requirements that institutions needed to comply with, and, therefore, in 2017, issued recommendations for outsourcing to cloud service providers. The recommendations were designed to feed into these revised guidelines to ensure that institutions have one single framework for all their outsourcing arrangements. Indeed, several aspects of the recommendations apply in general and are relevant beyond outsourcing

[17] 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.

[18] The term 'critical or important' is used in line with MiFID II and PSD2 and replaces the term 'material' that was used in the previous guidelines.

to cloud service providers, and those general aspects are reflected in these guidelines. However, where appropriate and relevant, a few specific requirements are applicable exclusively to cloud outsourcing.

40. The performance and quality of the cloud service provider's service delivery and the level of operational risk that it may cause to the outsourcing institution or payment institution are largely determined by the ability of the cloud service provider to appropriately protect the confidentiality, integrity and availability of data (in transit or at rest) and of the systems and processes that are used to process, transfer or store those data. Appropriate traceability mechanisms aimed at keeping records of technical and business operations are also key to detecting malicious attempts to breach the security of data and systems. Security expectations should take into account the need, on a risk-based approach, to protect the data and systems.

41. Cloud service providers often operate a geographically dispersed computing infrastructure that entails the regional and/or global distribution of data storage and processing; therefore, the security and privacy of data and their processing requires particular attention. Notwithstanding the requirements included in these guidelines, Union and national laws apply in this respect and, in particular with respect to any obligations or contractual rights referred to in these guidelines, attention should be paid to data protection rules and professional secrecy requirements.

42. With regard to sub-outsourcing, cloud outsourcing is more dynamic in nature than traditional outsourcing. There is a need for greater certainty about the conditions under which sub-contracting can take place, in particular in the case of cloud outsourcing.

43. The guidelines specify that sub-outsourcing requires *ex ante* notification to institutions and payment institutions in the case of outsourcing of critical or important functions. Institutions and payment institutions should always have the right to terminate the contract if planned changes to services, including such changes caused by sub-outsourcing, would have an adverse effect on the risk assessment of the outsourced services.

Supervision and concentration risks

44. It is of particular importance that competent authorities have a comprehensive overview of the outsourcing arrangements of institutions and payment institutions, as this enables them to exercise their supervisory powers. Institutions and payment institutions should therefore document all their outsourcing arrangements. In addition, institutions and payment institutions should inform competent authorities or engage with competent authorities in a dialogue regarding planned outsourcing arrangements, in particular with regard to critical or important functions. The final responsibility for outsourcing always remains with the institution or payment institution. To this end, the guidelines set out specific documentation requirements for institutions' and payment institutions' outsourcing arrangements.

45. Competent authorities need to identify the concentrations of outsourcing arrangements at service providers. The concentrations of outsourcing arrangements at service providers and as regards critical or important functions in particular may, if the provision of the service fails, lead to disruption of the provision of financial services by multiple institutions. If service providers,

e.g. in the area of IT or fintech, 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 market.

46. The need to monitor and manage concentration risk is particularly relevant for certain forms of IT outsourcing, including cloud outsourcing, which is dominated by a small number of highly dominant service providers. For instance, compared with more traditional forms of outsourcing offering tailor-made solutions to clients, cloud outsourcing services are much more standardised, which allows the services to be provided to a larger number of different clients in a much more automated manner and on a larger scale. Although cloud services can offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost-effectiveness, they also raise challenges in terms of data protection and location, security issues and concentration risk, not only from the point of view of individual institutions but also at industry level, as large suppliers of IT and cloud services can become a single point of failure when many institutions rely on them. Likewise, the development and increased use of financial technology providers requires specific attention.

EBA/GL/2019/02

25 February 2019

Guidelines on outsourcing

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010.[19] In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to which guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions and payment 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 25/04/20219. 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/2019/02'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

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

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

2. Subject matter, scope and definitions

Subject matter

5. These guidelines specify the internal governance arrangements, including sound risk management, that institutions, payment institutions and electronic money institutions should implement when they outsource functions, in particular with regard to the outsourcing of critical or important functions.

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[20], supervisory review and evaluation process (SREP), Article 9(3) of Directive (EU) 2015/2366[21], Article 5 (5) of Directive 2009/110/EC[22] by fulfilling their duty to monitor the continuous compliance of entities to which these guidelines are addressed with the conditions of their authorisation.

Addressees

7. These guidelines are addressed to competent authorities as defined in point 40 of Article 4(1) of Regulation (EU) No 575/2013[23], including the European Central Bank with regards to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013[24], to institutions as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013, to payment institutions as defined in Article 4(4) of Directive (EU) 2015/2366 and to electronic money institutions within the meaning of Article 2(1) of Directive 2009/110/EC. 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.

8. For the purpose of these guidelines, any reference to 'payment institutions' includes 'electronic money institutions' and any reference to 'payment services' includes 'issuing of electronic money'.

[20] 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.

[21] 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.

[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.

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

[24] Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions.

Scope of application

9. Without prejudice to Directive 2014/65/EU[25] and Commissions Delegated Regulation (EU) 2017/565[26] (which contains requirements regarding outsourcing by institutions 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 should comply with these guidelines on a solo basis, sub-consolidated basis and consolidated basis. The application on a solo 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 this Directive and 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.

10. 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.

11. Competent authorities responsible for the supervision of institutions, payment institutions and electronic money institutions should comply with these guidelines.

Definitions

12. Unless otherwise specified, terms used and defined in Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive 2009/110/EC, Directive (EU) 2015/2366 and the EBA Guidelines on internal governance[27] have the same meaning in these guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

Outsourcing	means an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself.

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

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

[27] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

Function	means any processes, services or activities.
Critical or important function[28]	means any function that is considered critical or important as set out in Section 4 of these guidelines.
Sub-outsourcing	means a situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider.[29]
Service provider	means a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.
Cloud services	means services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Public cloud	means cloud infrastructure available for open use by the general public.
Private cloud	means cloud infrastructure available for the exclusive use by a single institution or payment institution.
Community cloud	means cloud infrastructure available for the exclusive use by a specific community of institutions or payment institutions, including several institutions of a single group.
Hybrid cloud	means cloud infrastructure that is composed of two or more distinct cloud infrastructures.
Management body	means an institution's or payment institution's body or bodies, which are appointed in accordance with national law, which are empowered to set the institution's or payment institution'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 institution or payment institution and the directors and persons responsible for the management of the payment institution.

[28] The wording 'critical or important function' is based on the wording used under Directive 2014/65/EU (MiFID II) and Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II and is used only for the purpose of outsourcing; it is not related to the definition of 'critical functions' for the purpose of the recovery and resolution framework as defined under Article 2(1)(35) of Directive 2014/59/EU (BRRD).

[29] For the assessment, the provisions in Section 3 apply; sub-outsourcing has also been referred to in other EBA documents as a 'chain of outsourcing' or 'chain-outsourcing'.

3. Implementation

Date of application

13. With the exception of paragraph 63 (b), these guidelines apply from 30 September 2019 to all outsourcing arrangements entered into, reviewed or amended on or after this date. Paragraph 63 (b) applies from 31 December 2021.

14. Institutions and payment institutions should review and amend accordingly existing outsourcing arrangements with a view to ensuring that these are compliant with these guidelines.

15. Where the review of outsourcing arrangements of critical or important functions is not finalised by 31 December 2021, institutions and payment institutions should inform their competent authority of that fact, including the measures planned to complete the review or the possible exit strategy.

Transitional provisions

16. Institutions and payment institutions should complete the documentation of all existing outsourcing arrangements, other than for outsourcing arrangements to cloud service providers, in line with these guidelines following the first renewal date of each existing outsourcing arrangement, but by no later than 31 December 2021.

Repeal

17. The Committee of European Banking Supervisors (CEBS) guidelines on outsourcing of 14 December 2006 and the EBA recommendations on outsourcing to cloud service providers[30] are repealed with effect from 30 September 2019.

[30] Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).

4. Guidelines on outsourcing

Title I – Proportionality: group application and institutional protection schemes

1 Proportionality

18. Institutions, payment institutions 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 outsourcing, are consistent with the individual risk profile, the nature and business model of the institution or payment institution, and the scale and complexity of their activities so that the objectives of the regulatory requirements are effectively achieved.

19. When applying the requirements set out in these guidelines, institutions and payment institutions should take into account the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function and the potential impact of the outsourcing on the continuity of their activities.

20. When applying the principle of proportionality, institutions, payment institutions [31] and competent authorities should take into account the criteria specified in Title I of the EBA Guidelines on internal governance in line with Article 74(2) of Directive 2013/36/EU.

2 Outsourcing by groups and institutions that are members of an institutional protection scheme

21. In accordance with Article 109 (2) of Directive2013/36/EU, these guidelines should also apply on a sub-consolidated and consolidated basis, taking into account the prudential scope of consolidation.[32] For this purpose, the EU parent undertakings or the parent undertaking in a Member State should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries, including payment institutions, are consistent, well integrated and adequate for the effective application of these guidelines at all relevant levels.

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

[32] Please refer to Article 4(1) points (47) and (48) of Regulation (EU) No 575/2013 regarding the scope of consolidation.

22. Institutions and payment institutions, in accordance with paragraph 21, and institutions that, as members of an institutional protection scheme, use centrally provided governance arrangements should comply with the following:

    a. where those institutions or payment institutions have outsourcing arrangements with service providers within the group or the institutional protection scheme [33], the management body of those institutions or payment institutions retains, also for these outsourcing arrangements, full responsibility for compliance with all regulatory requirements and the effective application of these guidelines;

    b. where those institutions or payment institutions outsource the operational tasks of internal control functions to a service provider within the group or the institutional protection scheme, for the monitoring and auditing of outsourcing arrangements, institutions should ensure that, also for these outsourcing arrangements, those operational tasks are effectively performed, including through the receiving of appropriate reports.

23. In addition to paragraph 22, institutions and payment institutions 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 outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), institutions and payment institutions should ensure that, at least for outsourced critical or important functions, both independent monitoring of the service provider and appropriate oversight by each institution or payment institution is possible, including by receiving, at least annually and upon request from the centralised monitoring function, reports that include, at least, a summary of the risk assessment and performance monitoring. In addition, institutions and payment institutions should receive from the centralised monitoring function a summary of the relevant audit reports for critical or important outsourcing and, upon request, the full audit report;

    b. institutions and payment institutions should ensure that their management body will be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes;

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

c. where those institutions and payment institutions within the group, institutions affiliated to a central body or institutions that are part of an institutional protection scheme rely on a central pre-outsourcing assessment of outsourcing arrangements, as referred to in Section 12, each institution and payment institution 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 outsourcing arrangements, as referred to in Section 11, is established and maintained centrally within a group or institutional protection scheme, competent authorities, all institutions and payment institutions should be able to obtain their individual register without undue delay. This register should include all outsourcing arrangements, including outsourcing arrangements with service providers inside that group or institutional protection scheme;

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

24. 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.

25. Institutions and payment institutions that are subsidiaries of an EU parent undertaking or of a parent undertaking in a Member State to which no waivers have been granted on the basis of 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 outsourcing arrangements

3 Outsourcing

26. Institutions and payment institutions should establish whether an arrangement with a third party falls under the definition of outsourcing. Within this assessment, consideration should be given to whether the function (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider and whether this function (or part thereof) would normally fall within the scope of functions that would or could realistically be performed by institutions or payment institutions, even if the institution or payment institution has not performed this function in the past itself.

27. Where an arrangement with a service provider covers multiple functions, institutions and payment institutions should consider all aspects of the arrangement within their assessment, e.g. if the service provided includes the provision of data storage hardware and the backup of data, both aspects should be considered together.

28. As a general principle, institutions and payment institutions should not consider the following as outsourcing:

    a. a function that is legally required to be performed by a service provider, e.g. statutory audit;

    b. market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);

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

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

    e. global financial messaging infrastructures that are subject to oversight by relevant authorities;

    f. correspondent banking services; and

    g. the acquisition of services that would otherwise not be undertaken by the institution or payment institution (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line).

4 Critical or important functions

29. Institutions and payment institutions should always consider a function as critical or important in the following situations:[34]

    a. where a defect or failure in its performance would materially impair:

        i. their continuing compliance with the conditions of their authorisation or its other obligations under Directive 2013/36/EU, Regulation (EU) No 575/2013,

[34] See also Article 30 Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.

Directive 2014/65/EU, Directive (EU) 2015/2366 and Directive 2009/110/EC and their regulatory obligations;

ii. their financial performance; or

iii. the soundness or continuity of their banking and payment services and activities;

b. when operational tasks of internal control functions are outsourced, unless the assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the effectiveness of the internal control function;

c. when they intend to outsource functions of banking activities or payment services to an extent that would require authorisation[35] by a competent authority, as referred to in Section 12.1.

30. In the case of institutions, particular attention should be given to the assessment of the criticality or importance of functions if the outsourcing concerns functions related to core business lines and critical functions as defined in Article 2(1)(35) and 2(1)(36) of Directive 2014/59/EU[36] and identified by institutions using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778.[37] Functions that are necessary to perform activities of core business lines or critical functions should be considered as critical or important functions for the purpose of these guidelines, unless the institution's assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the operational continuity of the core business line or critical function.

31. When assessing whether an outsourcing arrangement relates to a function that is critical or important, institutions and payment institutions should take into account, together with the outcome of the risk assessment outlined in Section 12.2, at least the following factors:

a. whether the outsourcing arrangement is directly connected to the provision of banking activities or payment services[38] for which they are authorised;

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

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

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

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

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

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

   ii. business continuity and operational resilience;

   iii. operational risk, including conduct, information and communication technology (ICT) and legal risks;

   iv. reputational risks;

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

c. the potential impact of the outsourcing arrangement on their ability to:

   i. identify, monitor and manage all risks;

   ii. comply with all legal and regulatory requirements;

   iii. conduct appropriate audits regarding the outsourced function;

d. the potential impact on the services provided to its clients;

e. all outsourcing arrangements, the institution's or payment institution's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area;

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

g. the possibility that the proposed outsourcing arrangement might be scaled up without replacing or revising the underlying agreement;

h. the ability to transfer the proposed outsourcing arrangement to another service provider, 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');

i. the ability to reintegrate the outsourced function into the institution or payment institution, if necessary or desirable;

j. the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the institution or payment institution and its clients, including but not limited to compliance with Regulation (EU) 2016/679[39] .

[39] 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).

Title III – Governance framework

5 Sound governance arrangements and third-party risk

32. As part of the overall internal control framework,[40] including internal control mechanisms,[41] institutions and payment institutions should have a holistic institution-wide risk management framework extending across all business lines and internal units. Under that framework, institutions and payment institutions should identify and manage all their risks, including risks caused by arrangements with third parties. The risk management framework should also enable institutions and payment institutions to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented, including with regard to cyber risks.[42]

33. Institutions and payment institutions, taking into account the principle of proportionality in line with Section 1, should identify, assess, monitor and manage all risks resulting from arrangements with third parties to which they are or might be exposed, regardless of whether or not those arrangements are outsourcing arrangements. The risks, in particular the operational risks, of all arrangements with third parties, including the ones referred to in paragraphs 26 and 28, should be assessed in line with Section 12.2.

34. Institutions and payment institutions should ensure that they comply with all requirements under Regulation (EU) 2016/679, including for their third-party and outsourcing arrangements.

6 Sound governance arrangements and outsourcing

35. The outsourcing of functions cannot result in the delegation of the management body's responsibilities. Institutions and payment institutions remain fully responsible and accountable for complying with all of their regulatory obligations, including the ability to oversee the outsourcing of critical or important functions.

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

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

    b. the internal organisation of the institution or the payment institution;

[40] Institutions should refer to Title V of the EBA guidelines on internal governance.

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

[42] See also EBA guidelines on ICT and security risk management (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) and G7 fundamental elements for third-party cyber risk management in the financial sector (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

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

d. the setting of the institution's or payment institution'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 institution or payment institution, including the management of all risks associated with outsourcing; and

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

37. Outsourcing should not lower the suitability requirements applied to the members of an institution's management body, directors and persons responsible for the management of the payment institution and key function holders. Institutions and payment institutions should have adequate competence and sufficient and appropriately skilled resources to ensure appropriate management and oversight of outsourcing arrangements.

38. Institutions and payment institutions should:

a. clearly assign the responsibilities for the documentation, management and control of outsourcing arrangements;

b. allocate sufficient resources to ensure compliance with all legal and regulatory requirements, including these guidelines and the documentation and monitoring of all outsourcing arrangements;

c. taking into account Section 1 of these guidelines, establish an outsourcing function or designate a senior staff member who is directly accountable to the management body (e.g. a key function holder of a control function) and responsible for managing and overseeing the risks of outsourcing arrangements as part of the institutions internal control framework and overseeing the documentation of outsourcing arrangements. Small and less complex institutions or payment institutions should at least ensure a clear division of tasks and responsibilities for the management and control of outsourcing arrangements and may assign the outsourcing function to a member of the institution's or payment institution's management body.

39. Institutions and payment institutions 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[43] at all times, including the management body effectively carrying out its responsibilities as set out in paragraph 36 of these guidelines;

[43] 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

b. retain a clear and transparent organisational framework and structure that enables them to ensure compliance with legal and regulatory requirements;

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

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

40. When outsourcing, institutions and payment institutions should at least ensure that:

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

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

c. the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (fintech);

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

e. an appropriate flow of relevant information with service providers is maintained;

f. with regard to the outsourcing of 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 service providers;

   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.

authorisation of credit institutions (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

For payment institutions, please refer to the EBA guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and electronic money institutions and for the registration of account information service providers (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

7 Outsourcing policy

41. The management body of an institution or payment institution [44] that has outsourcing arrangements in place or plans on entering into such arrangements should approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis. For institutions, the outsourcing policy should be in accordance with Section 8 of the EBA's Guidelines on internal governance and, in particular, should take into account the requirements set out in Section 18 (new products and significant changes) of those guidelines. Payment institutions may also align their policies with Sections 8 and 18 of the EBA Guidelines on internal governance.

42. The policy should include the main phases of the life cycle of outsourcing arrangements and define the principles, responsibilities and processes in relation to outsourcing. In particular, the policy should cover at least:

    a. the responsibilities of the management body in line with paragraph 36, including its involvement, as appropriate, in the decision-making on outsourcing of critical or important functions;

    b. the involvement of business lines, internal control functions and other individuals in respect of outsourcing arrangements;

    c. the planning of outsourcing arrangements, including:

        i. the definition of business requirements regarding outsourcing arrangements;

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

        iii. risk identification, assessment and management in accordance with Section 12.2;

        iv. due diligence checks on prospective service providers, including the measures required under Section 12.3;

        v. procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with Section 8;

        vi. business continuity planning in accordance with Section 9;

        vii. the approval process of new outsourcing arrangements;

[44] 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

d. the implementation, monitoring and management of outsourcing arrangements, including:

   i. the ongoing assessment of the service provider's performance in line with Section 14;

   ii. the procedures for being notified and responding to changes to an outsourcing arrangement or service provider (e.g. to its financial position, organisational or ownership structures, sub-outsourcing);

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

   iv. the renewal processes;

e. the documentation and record-keeping, taking into account the requirements in Section 11;

f. the exit strategies and termination processes, including a requirement for a documented exit plan for each critical or important function to be outsourced where such an exit is considered possible taking into account possible service interruptions or the unexpected termination of an outsourcing agreement.

43. The outsourcing policy should differentiate between the following:

a. outsourcing of critical or important functions and other outsourcing arrangements;

b. outsourcing to service providers that are authorised by a competent authority and those that are not;

c. intragroup outsourcing arrangements, outsourcing arrangements within the same institutional protection scheme (including entities fully owned individually or collectively by institutions within the institutional protection scheme) and outsourcing to entities outside the group; and

d. outsourcing to service providers located within a Member State and third countries.

44. Institutions and payment institutions should ensure that the policy covers the identification of the following potential effects of critical or important outsourcing arrangements and that these are taken into account in the decision-making process:

a. the institution's risk profile;

b. the ability to oversee the service provider and to manage the risks;

c. the business continuity measures; and

d. the performance of their business activities.

8 Conflicts of interests

45. Institutions, in line with Title IV, Section 11, of the EBA Guidelines on internal governance,[45] and payment institutions should identify, assess and manage conflicts of interests with regard to their outsourcing arrangements.

46. Where outsourcing creates material conflicts of interest, including between entities within the same group or institutional protection scheme, institutions and payment institutions need to take appropriate measures to manage those conflicts of interest.

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

9 Business continuity plans

48. Institutions, in line with the requirements under Article 85(2) of Directive 2013/36/EU and Title VI of the EBA Guidelines on internal governance,[46] and payment institutions should have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions. Institutions and payment institutions within a group or institutional protection scheme may rely on centrally established business continuity plans regarding their outsourced functions.

49. Business continuity plans should take into account the possible event that the quality of the provision of the outsourced critical or important function deteriorates to an unacceptable level or fails. Such plans should also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, political risks in the service provider's jurisdiction.

[45] Payment institutions may also align their policies with those guidelines.

[46] Available under: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

10 Internal audit function

50. The internal audit function's[47] activities should cover, following a risk-based approach, the independent review of outsourced activities. The audit plan[48] and programme should include, in particular, the outsourcing arrangements of critical or important functions.

51. With regard to the outsourcing process, the internal audit function should at least ascertain:

    a. that the institution's or payment institution's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk strategy and the decisions of the management body;

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

    c. the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the institution's risk strategy;

    d. the appropriate involvement of governance bodies; and

    e. the appropriate monitoring and management of outsourcing arrangements.

11 Documentation requirements

52. As part of their risk management framework, institutions and payment institutions should maintain an updated register of information on all outsourcing arrangements at the institution and, where applicable, at sub-consolidated and consolidated levels, as set out in Section 2, and should appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. Taking into account national law, institutions should maintain the documentation of ended outsourcing arrangements within the register and the supporting documentation for an appropriate period.

53. Taking into account Title I of these guidelines, and under the conditions set out in paragraph 23(d), for institutions and payment institutions within a group, institutions permanently affiliated to a central body or institutions that are members of the same institutional protection scheme, the register may be kept centrally.

[47] 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-) and payment institutions should refer to Guideline 5 of the EBA guidelines on the authorisation of payment institutions (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[48] 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

54. The register should include at least the following information for all existing outsourcing arrangements:

    a. a reference number for each outsourcing arrangement;

    b. the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the institution or payment institution;

    c. a brief description of the outsourced function, including the data that are outsourced and whether or not personal data (e.g. by providing a yes or no in a separate data field) have been transferred or if their processing is outsourced to a service provider;

    d. a category assigned by the institution or payment institution that reflects the nature of the function as described under point (c) (e.g. information technology (IT), control function), which should facilitate the identification of different types of arrangements;

    e. the name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any);

    f. the country or countries where the service is to be performed, including the location (i.e. country or region) of the data;

    g. whether or not (yes/no) the outsourced function is considered critical or important, including, where applicable, a brief summary of the reasons why the outsourced function is considered critical or important;

    h. in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;

    i. the date of the most recent assessment of the criticality or importance of the outsourced function.

55. For the outsourcing of critical or important functions, the register should include at least the following additional information:

    a. the institutions, payment institutions and other firms within the scope of the prudential consolidation or institutional protection scheme, where applicable, that make use of the outsourcing;

    b. whether or not the service provider or sub-service provider is part of the group or a member of the institutional protection scheme or is owned by institutions or payment institutions within the group or is owned by members of an institutional protection scheme;

    c. the date of the most recent risk assessment and a brief summary of the main results;

d. the individual or decision-making body (e.g. the management body) in the institution or the payment institution that approved the outsourcing arrangement;

e. the governing law of the outsourcing agreement;

f. the dates of the most recent and next scheduled audits, where applicable;

g. where applicable, the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including the country where the sub-contractors are registered, where the service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored;

h. an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the institution or the payment institution or the impact of discontinuing the critical or important function;

i. identification of alternative service providers in line with point (h);

j. whether the outsourced critical or important function supports business operations that are time-critical;

k. the estimated annual budget cost.

56. Institutions and payment institutions should, upon request, make available to the competent authority either the full register of all existing outsourcing arrangements[49] or sections specified thereof, such as information on all outsourcing arrangements falling under one of the categories referred to in point (d) of paragraph 54 of these guidelines (e.g. all IT outsourcing arrangements). Institutions and payment institutions should provide this information in a processable electronic form (e.g. a commonly used database format, comma separated values).

57. Institutions and payment institutions should, upon request, make available to the competent authority all information necessary to enable the competent authority to execute the effective supervision of the institution or the payment institution, including, where required, a copy of the outsourcing agreement.

58. Institutions, without prejudice to Article 19(6) of Directive (EU) 2015/2366, and payment institutions should adequately inform competent authorities in a timely manner or engage in a supervisory dialogue with the competent authorities about the planned outsourcing of critical or important functions and/or where an outsourced function has become critical or important and provide at least the information specified in paragraph 54.

[49] 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

59. Institutions and payment institutions[50] should inform competent authorities in a timely manner of material changes and/or severe events regarding their outsourcing arrangements that could have a material impact on the continuing provision of the institutions' or payment institutions' business activities.

60. Institutions and payment institutions should appropriately document the assessments made under Title IV and the results of their ongoing monitoring (e.g. performance of the service provider, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).

Title IV – Outsourcing process

12 Pre-outsourcing analysis

61. Before entering into any outsourcing arrangement, institutions and payment institutions should:

    a. assess if the outsourcing arrangement concerns a critical or important function, as set out in Title II;

    b. assess if the supervisory conditions for outsourcing set out in Section 12.1 are met;

    c. identify and assess all of the relevant risks of the outsourcing arrangement in accordance with Section 12.2;

    d. undertake appropriate due diligence on the prospective service provider in accordance with Section 12.3;

    e. identify and assess conflicts of interest that the outsourcing may cause in line with Section 8.

12.1 Supervisory conditions for outsourcing

62. Institutions and payment institutions should ensure that the outsourcing of functions of banking activities[51] or payment services, 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 service provider located in the same or another Member State takes place only if one of the following conditions is met:

[50] See also the EBA Guidelines on major incident reporting under PSD2, available under: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

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

a. the service provider is authorised or registered by a competent authority to perform such banking activities or payment services; or

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

63. Institutions and payment institutions should ensure that the outsourcing of functions of banking activities or payment services, 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 service provider located in a third country takes place only if the following conditions are met:

a. the service provider is authorised or registered to provide that banking activity or payment 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 institution and the supervisory authorities responsible for the supervision of the service provider; and

c. the cooperation agreement referred to in point (b) should ensure 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, Regulation (EU) No 575/2013, Directive (EU) 2015/2366 and Directive 2009/110/EC;

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 and Directive 2009/110/EC; 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.

12.2 Risk assessment of outsourcing arrangements

64. Institutions and payment institutions should assess the potential impact of outsourcing arrangements on their operational risk, should take into account the assessment results when deciding if the function should be outsourced to a service provider and should take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.

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

66. Within the risk assessment, institutions and payments institutions should also take into account the expected benefits and costs of the proposed outsourcing arrangement, including weighing any risks that may be reduced or better managed against any risks that may arise as a result of the proposed outsourcing arrangement, taking into account at least:

    a. concentration risks, including from:

        i. outsourcing to a dominant service provider that is not easily substitutable; and

        ii. multiple outsourcing arrangements with the same service provider or closely connected service providers;

    b. the aggregated risks resulting from outsourcing several functions across the institution or payment institution 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 service provider in distress or to take over its business operations; and

    d. the measures implemented by the institution or payment institution and by the service provider to manage and mitigate the risks.

67. Where the outsourcing arrangement includes the possibility that the service provider sub-outsources critical or important functions to other service providers, institutions and payment institutions should take into account:

a. the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider;

b. the risk that long and complex chains of sub-outsourcing reduce the ability of institutions or payment institutions to oversee the outsourced critical or important function and the ability of competent authorities to effectively supervise them.

68. When carrying out the risk assessment prior to outsourcing and during ongoing monitoring of the service provider's performance, institutions and payment institutions should, at least:

a. identify and classify the relevant functions and related data and systems as regards their sensitivity and required security measures;

b. conduct a thorough risk-based analysis of the functions and related data and systems that are being considered for outsourcing or have been outsourced and address the potential risks, in particular the operational risks, including legal, ICT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced services are or may be provided and where the data are or are likely to be stored;

c. consider the consequences of where the service provider 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;

ii. the law enforcement provisions in place; and

iii. the insolvency law provisions that would apply in the event of a service provider's failure and any constraints that would arise in respect of the urgent recovery of the institution's or payment institution's data in particular;

e. define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the intended outsourcing. Institutions and payment institutions should also consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture;

f. consider whether the service provider is a subsidiary or parent undertaking of the institution, is included in the scope of accounting consolidation or is a member of or owned by institutions that are members of an institutional protection scheme and, if

so, the extent to which the institution controls it or has the ability to influence its actions in line with Section 2.

12.3 Due diligence

69. Before entering into an outsourcing arrangement and considering the operational risks related to the function to be outsourced, institutions and payment institutions should ensure in their selection and assessment process that the service provider is suitable.

70. With regard to critical and important functions, institutions and payment institutions should ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, IT, financial), the organisational structure and, 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 draft contract.

71. Additional factors to be considered when conducting due diligence on a potential service provider include, but are not limited to:

    a. its business model, nature, scale, complexity, financial situation, ownership and group structure;

    b. the long-term relationships with service providers that have already been assessed and perform services for the institution or payment institution;

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

    d. whether or not the service provider is supervised by competent authorities.

72. Where outsourcing involves the processing of personal or confidential data, institutions and payment institutions should be satisfied that the service provider implements appropriate technical and organisational measures to protect the data.

73. Institutions and payment institutions should take appropriate steps to ensure that service providers act in a manner consistent with their values and code of conduct. In particular, with regard to service providers located in third countries and, if applicable, their sub-contractors, institutions and payment institutions should be satisfied that the service provider acts in an ethical and socially responsible manner and adheres to international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.

13 Contractual phase

74. The rights and obligations of the institution, the payment institution and the service provider should be clearly allocated and set out in a written agreement.

75. The outsourcing agreement for critical or important functions should set out at least:

    a. a clear description of the outsourced function to be provided;

    b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution or payment institution;

    c. the governing law of the agreement;

    d. the parties' financial obligations;

    e. whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in Section 13.1 that the sub-outsourcing is subject to;

    f. the location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the institution or payment institution if the service provider proposes to change the location(s);

    g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Section 13.2;

    h. the right of the institution or payment institution to monitor the service provider's performance on an ongoing basis;

    i. the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;

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

    k. whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

l. the requirements to implement and test business contingency plans;

m. provisions that ensure that the data that are owned by the institution or payment institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;

n. the obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them;

o. for institutions, 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;

p. the unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, as specified in Section 13.3;

q. termination rights, as specified in Section 13.4.

13.1 Sub-outsourcing of critical or important functions

76. The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted.

77. If sub-outsourcing of critical or important functions is permitted, institutions and payment institutions should determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.

78. If sub-outsourcing of critical or important functions is permitted, the written agreement should:

a. specify any types of activities that are excluded from sub-outsourcing;

b. specify the conditions to be complied with in the case of sub-outsourcing;

c. specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the institution or payment institution are continuously met;

d. require the service provider to obtain prior specific or general written authorisation from the institution or payment institution before sub-outsourcing data;[52]

[52] See Article 28 of Regulation (EU) 2016/679.

e. include an obligation of the service provider to inform the institution or payment institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set should allow the outsourcing institution or payment institution at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;

f. ensure, where appropriate, that the institution or payment institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;

g. ensure that the institution or payment institution has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the institution or payment institution or where the service provider sub-outsources without notifying the institution or payment institution.

79. Institutions and payment institutions should agree to sub-outsourcing only if the sub-contractor undertakes to:

a. comply with all applicable laws, regulatory requirements and contractual obligations; and

b. grant the institution, payment institution and competent authority the same contractual rights of access and audit as those granted by the service provider.

80. Institutions and payment institutions should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the institution or payment institution. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in paragraph 79 would not be met, the institution or payment institution should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.

13.2 Security of data and systems

81. Institutions and payment institutions should ensure that service providers, where relevant, comply with appropriate IT security standards.

82. Where relevant (e.g. in the context of cloud or other ICT outsourcing), institutions and payment institutions should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.

83. In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, institutions and payment institutions should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.

84. Without prejudice to the requirements under the Regulation (EU) 2016/679, institutions and payment institutions, when outsourcing (in particular to third countries), should take into account differences in national provisions regarding the protection of data. Institutions and payment institutions should ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the institution or payment institution (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).

13.3 Access, information and audit rights

85. Institutions and payment institutions should ensure within the written outsourcing arrangement that the internal audit function is able to review the outsourced function using a risk-based approach.

86. Regardless of the criticality or importance of the outsourced function, the written outsourcing arrangements between institutions and service providers 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 service providers located in a Member State and should also ensure those rights with regard to service providers located in third countries.

87. With regard to the outsourcing of critical or important functions, institutions and payment institutions should ensure within the written outsourcing agreement that the service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:

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

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

88. For the outsourcing of functions that are not critical or important, institutions and payment institutions should ensure the access and audit rights as set out in paragraph 87 (a) and (b) and

Section 13.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. Institutions and payment institutions should take into account that functions may become critical or important over time.

89. Institutions and payment institutions should ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, competent authorities or third parties appointed by them to exercise these rights.

90. Institutions and payment institutions 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.[53]

91. Without prejudice to their final responsibility regarding outsourcing arrangements, institutions and payment institutions may use:

    a. pooled audits organised jointly with other clients of the same service provider, 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 service provider;

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

92. For the outsourcing of critical or important functions, institutions and payment institutions should assess whether third-party certifications and reports as referred to in paragraph 91(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.

93. Institutions and payment institutions should make use of the method referred to in paragraph 91(b) only if they:

    a. are satisfied with the audit plan for the outsourced function;

    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 institution or payment institution 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;

[53] 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

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 outsourcing of critical or important functions.

94. In line with the EBA Guidelines on ICT risk assessment under the SREP, institutions should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.[54] Taking into account Title I, payment institutions should also have internal ICT control mechanisms, including ICT security control and mitigation measures.

95. Before a planned on-site visit, institutions, payment institutions, competent authorities and auditors or third parties acting on behalf of the institution, payment institution or competent authorities should provide reasonable notice to the service provider, 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.

96. 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.

97. Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the institution or payment institution 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 institution or payment institution reviewing third-party certifications or audits carried out by service providers.

[54] See also EBA Guidelines on ICT risk: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

13.4 Termination rights

98. The outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate the arrangement, in accordance with applicable law, including in the following situations:

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

    b. where impediments capable of altering the performance of the outsourced function are identified;

    c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);

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

    e. where instructions are given by the institution's or payment institution's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the institution or payment institution.

99. The outsourcing arrangement should facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the institution or payment institution. To this end, the written outsourcing arrangement should:

    a. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the institution or payment institution, including the treatment of data;

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

    c. include an obligation of the service provider to support the institution or payment institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement.

14 Oversight of outsourced functions

100. Institutions and payment institutions should monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of critical or important functions, including that the availability, integrity and security of data and information is

ensured. Where the risk, nature or scale of an outsourced function has materially changed, institutions and payment institutions should reassess the criticality or importance of that function in line with Section 4.

101. Institutions and payment institutions should apply due skill, care and diligence when monitoring and managing outsourcing arrangements.

102. Institutions should regularly update their risk assessment in accordance with Section 12.2and should periodically report to the management body on the risks identified in respect of the outsourcing of critical or important functions.

103. Institutions and payment institutions should monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account Section 12.2 of these guidelines.

104. Institutions and payment institutions should ensure, on an ongoing basis, that outsourcing arrangements, with the main focus being on outsourced critical or important functions, meet appropriate performance and quality standards in line with their policies by:

a. ensuring that they receive appropriate reports from service providers;

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

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

105. Institutions should take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, institutions and payment institutions should follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, institutions and payment institutions should take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.

15 Exit strategies

106. Institutions and payment institutions should have a documented exit strategy when outsourcing critical or important functions that is in line with their outsourcing policy and business continuity plans,[55] taking into account at least the possibility of:

[55] Institutions, in line with the requirements under Article 85(2) of Directive 2013/36/EU and Title VI of the EBA Guidelines on internal governance, and payment institutions should have appropriate business continuity plans in place with regard to the outsourcing of critical or important functions.

a. the termination of outsourcing arrangements;

b. the failure of the service provider;

c. 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;

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

107. Institutions and payment institutions should ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, they should:

a. develop and implement exit plans that are 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 an outsourced service to an alternative provider); and

b. identify alternative solutions and develop transition plans to enable the institution or payment institution to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the institution or payment institution 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.

108. When developing exit strategies, institutions and payment institutions should:

a. define the objectives of the exit strategy;

b. perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;

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

d. define success criteria for the transition of outsourced functions and data; and

e. define the indicators to be used for the monitoring of the outsourcing arrangement (as outlined under Section 14), including indicators based on unacceptable service levels that should trigger the exit.

Title V – Guidelines on outsourcing addressed to competent authorities

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

110. Competent authorities should be satisfied that they can effectively supervise institutions and payment institutions, including that institutions or payment institutions have ensured within their outsourcing arrangement that service providers are obliged to grant audit and access rights to the competent authority and the institution, in line with Section 13.3.

111. The analysis of institutions' outsourcing risks should be performed at least within the SREP or, with regard to payment institutions, as part of other supervisory processes, including ad-hoc requests, or during on-site inspections.

112. Further to the information recorded within the register, as referred to in Section 11, competent authorities may ask institutions and payment institutions for additional information, in particular for critical or important outsourcing arrangements, such as:

a. the detailed risk analysis;

b. whether the service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution or payment institution;

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

d. the resources and measures in place to adequately monitor the outsourced activities.

113. In addition to the information required under Section 11, competent authorities may require institutions and payment institutions to provide detailed information on any outsourcing arrangement, even if the function concerned is not considered critical or important.

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

a. whether institutions and payment institutions monitor and manage appropriately, in particular, critical or important outsourcing arrangements;

b. whether institutions and payment institutions have sufficient resources in place to monitor and manage outsourcing arrangements;

c. whether institutions and payment institutions identify and manage all relevant risks; and

d. whether institutions and payment institutions identify, assess and appropriately manage conflicts of interest with regard to outsourcing arrangements, e.g. in the case of intragroup outsourcing or outsourcing within the same institutional protection scheme.

115. Competent authorities should ensure that EU/EEA institutions and payment institutions are not operating as an 'empty shell', including situations where institutions 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.

116. Within their assessment, competent authorities should take into account all risks, in particular:[56]

a. the operational risks[57] posed by the outsourcing arrangement;

b. reputational risks;

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

d. concentration risks within the institution, including on a consolidated basis, caused by multiple outsourcing arrangements with a single service provider or closely connected service providers or multiple outsourcing arrangements within the same business area;

e. concentration risks at the sector level, e.g. where multiple institutions or payment institutions make use of a single service provider or a small group of service providers;

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

g. conflicts of interest between the institution and the service provider.

117. Where concentration risks are identified, competent authorities should monitor the development of such risks and evaluate both their potential impact on other institutions and payment institutions and the stability of the financial market; competent authorities should inform, where appropriate, the resolution authority about new potentially critical functions[58] that have been identified during this assessment.

[56] 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

[57] See also the EBA Guidelines on ICT risk: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

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

118. Where concerns are identified that lead to the conclusion that an institution or payment institution 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 outsourced functions or requiring exit from one or more outsourcing arrangements. In particular, taking into account the need of the institution or payment institution to operate on a continuous basis, the cancellation of contracts could be required if the supervision and enforcement of regulatory requirements cannot be ensured by other measures.

119. Competent authorities should be satisfied that they are able to perform effective supervision, in particular when institutions and payment institutions outsource critical or important functions that are undertaken outside the EU/EEA.

5. Accompanying documents

5.1 Draft cost-benefit analysis/impact assessment

Article 16(2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) (the EBA Regulation) provides that the EBA should carry out an analysis of 'the potential related costs and benefits' of any guidelines it develops. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.

A. Problem identification

The CEBS guidelines on outsourcing, published in 2006, were applicable exclusively to credit institutions and needed to be replaced by EBA guidelines applicable to all institutions and payment institutions to establish a more harmonised framework for the outsourcing arrangements of all financial institutions in the scope of the EBA's action. The update was also necessary to take into account changes within EU legislation. In addition, outsourcing to third countries may change in volume after the UK's notification of its intention to leave the EU. Furthermore, the scope and nature of outsourcing arrangements have changed over time and, in particular, the outsourcing of IT processes and infrastructures became more common. High concentrations of IT services at a limited number of service providers have the potential to lead to risks for the stability of the financial market, particularly if no additional safeguards would be implemented.

B. Policy objectives

To ensure a level playing field and to meet the requirements of the CRD, PSD2 and EMD, the EBA is now updating the guidelines issued by its predecessor to establish one common framework for the outsourcing of all financial institutions within the scope of the EBA's action.

To cater for the principle of proportionality and in accordance with the approach taken in the MiFID II and PSD2, the guidelines require that the outsourcing of critical or important functions be identified and impose stricter requirements on such outsourcing compared with other outsourcing arrangements.

The guidelines aim to clarify the supervisory expectations regarding outsourcing to service providers, including service providers located in third countries, to ensure that outsourcing is performed in an orderly manner and not performed to an extent that would lead to the setting up of empty shells that no longer have the substance to remain authorised.

The guidelines aim to ensure that competent authorities are able to identify concentrations of outsourcing arrangements at service providers based on documentation provided by institutions and payment institutions, to identify and manage risks to the stability of the financial system.

C. Baseline scenario

Outsourcing requirements are currently specified in the CEBS guidelines on outsourcing. In addition, the EBA has published a recommendation on outsourcing to cloud service providers. Outsourcing by firms performing investment services is regulated under MiFID II and Commission Delegated Regulation (EU) 2017/565. Outsourcing by payment institutions is regulated under the PSD2.

Institutions should comply with the CRD. Article 74 CRD requires institutions to have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks they are or they might be exposed to and adequate internal control mechanisms. The EBA Guidelines on internal governance sufficiently specify the requirements, including the need for institutions to have appropriate outsourcing policies (see Section 8 of the guidelines); in addition, outsourcing needs to be approved as part of the institution's new product approval and change processes (see Section 18 of the guidelines).

Article 76 CRD sets out requirements for the involvement of the management body in risk management and Article 88 CRD sets out the responsibilities of the management body regarding governance arrangements; in both cases, the requirements are relevant for outsourced activities.

According to Article 11 PSD2, competent authorities should grant an authorisation only if, taking into account the need to ensure the sound and prudent management of a payment institution, the payment institution has robust governance arrangements for its payment services business, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective procedures to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures; those arrangements, procedures and mechanisms must be comprehensive and proportionate to the nature, scale and complexity of the payment services provided by the payment institution.

Institutions and payment institutions must ensure that sensitive data, including personal data, is adequately protected and kept confidential. Institutions must comply with the GDPR.

All of the above forms the baseline scenario of the impact assessment, which focuses only on the additional costs and benefits created by the guidelines on outsourcing.

D. Options considered

1) Scope of application

Option A: applying the guidelines only to credit institutions (as in the previous CEBS guidelines).

Option B: applying the guidelines to all credit institutions and investment firms (both referred to as 'institutions') that are subject to the CRD, payment institutions that are subject to the PSD2 and electronic money institutions subject to the EMD (both referred to as 'payment institutions').

Firms providing investment services are subject to the specific provisions on outsourcing included in MiFID II and Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II.

MiFID II and PSD2 already set out a framework for outsourcing. An application limited to credit institutions and their banking activities would be sufficient to complete the framework on outsourcing. However, such an approach (Option A) would potentially lead to inconsistencies between the different frameworks and to a situation in which there is not a level playing field between investment firms, payment institutions, electronic money institutions and credit institutions. In particular, credit institutions would need to implement separate arrangements for the different types of activities.

The EBA's scope of action covers not only credit institutions and investment firms subject to the CRD, but also payment and electronic money institutions. While the guidelines would cover all those institutions and payment institutions, the guidelines would not directly be addressed to account information service providers registered only for this service, credit intermediaries or non-bank creditors. Outsourcing arrangements between institutions and payment institutions and such entities are within the scope of the guidelines, as the requirements are addressed to institutions and payment institutions. Such an approach (Option B), if the requirements are aligned with the provisions within MiFID II and the supplemental Commission Delegated Regulation and within the PSD2, would establish a level playing field between different types of financial institutions and ensure that credit institutions can implement one framework for the outsourcing of their activities governed by different directives. The specific aspects of intragroup outsourcing and outsourcing within institutional protection schemes will be considered.

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 the regular implementation period of six months and setting out transitional arrangements to ensure that institutions can review contracts, update the assessment of the criticality or importance of outsourcing and set up a register and update the documentation in line with the requirements.

Option B1: setting a fixed transitional period of around two years to review contracts, perform assessments and complete the register.

Option B2: setting a period of around two years (other than for outsourcing arrangements to cloud service providers, for which the EBA recommendation already applies), but requiring documentation and assessments to be updated if existing outsourcing arrangements are renewed during that period. For critical or important arrangements, closer supervisory attention should be applied and, after the transitional period, their reassessment should be monitored.

All options would be effective to achieve the desired prudential outcome to have all outsourcing arrangements documented in a way that differentiates between critical and important outsourcing, sets out a framework for such outsourcing and allows for the submission of a register to competent authorities.

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

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

Option B2 would lead to a faster update than Option B1 for arrangements that are renewed during the transitional period, but without additional burden, as an assessment of renewed outsourcing arrangements would include the assessment of the related risks. Updating the documentation in that context would be possible without causing material additional costs. Option B2 would have some impact on the available time frame for the development of a database that could hold the register. However, for this task, the regular implementation period should be sufficient. Additional scrutiny would be applied to critical or important outsourcing arrangements that are updated only after the transitional period. While this would lead to additional costs for competent authorities for the monitoring of the transition, it would reduce the costs of institutions, as the time pressure for renegotiation of contracts or, in some cases, exit from arrangements (where there is no renegotiation possible that ensures compliance with the guidelines) would be reduced.

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

3) Definition of outsourcing and the approach regarding the outsourcing of critical and important functions

Option A: relying on the definition provided in MiFID II and the Commission Delegated Regulation and the approach to set more detailed requirements for the outsourcing of critical and important functions.

Option B: the same as Option A, but also setting a lighter framework for other outsourcing arrangements.

Option C: creating a more narrow definition for the outsourcing of banking services.

Using a common definition (Option A) ensures that institutions can implement a single framework for outsourcing regarding all of their activities and develop a good understanding of the scope of outsourcing. A focus on the outsourcing of critical or important functions should reduce the administrative costs of applying the guidelines. However, the assessment of the criticality or

importance includes judgemental elements and therefore institutions, payment institutions and competent authorities may sometimes disagree regarding the assessment result. Retroactively introducing safeguards for the outsourcing of critical or important functions, also in cases where the assessment changes over time, could lead to additional costs and situations where necessary contractual changes are difficult to agree on. In addition, the overall impact of outsourcing arrangements that are themselves not critical or important might become relevant for the supervision of an institution.

Under Option B, the impact described under Option A would apply; in addition, some requirements for all outsourcing would be imposed, taking into account the principle of proportionality. This would lead to only a minor additional administrative burden, as institutions would already need to have in place some processes to manage all of their arrangements with third parties. In any case, also for other outsourcing arrangements, institutions would already need to apply sound processes and would need to document the arrangements to ensure that they have robust governance arrangements in place. Having guidelines in place that specify the regulatory minimum expectations for such non-critical or non-important arrangements would provide a higher level of legal certainty. Costs for adjustments of internal processes should be minor. It would be ensured that the outsourcing process would be subject to a prescribed set of controls, which should mitigate the additional measures that would need to be taken if an outsourcing arrangement became critical or important over time, e.g. because of the scalability of the arrangement.

A narrower definition of outsourcing (Option C) for banking activities would limit the number of outsourcing arrangements and this would, at first sight, reduce the administrative costs of applying the guidelines. However, the framework should ensure a sufficient focus on the outsourcing of critical or important functions and, by doing so, this would limit the administrative burden. A different definition would require different frameworks for different activities (e.g. banking versus investment services) and would lead to challenges in their application, as some arrangements affect banking, but also investment and payment services (e.g. underlying IT infrastructures). Therefore, Option C is not effective.

Option B has been retained.

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

Option A: the guidelines should not specify such requirements, as the EBA Guidelines on internal governance are sufficient.

Option B: the guidelines should specify the additional aspects that are specific in terms of outsourcing.

The guidelines on internal governance do not apply to payment institutions; therefore, Option A would be less effective than Option B, even if one were to take into account the fact that the prudential risks within such institutions would be low compared with institutions that are subject to the CRD. This option would also not provide legal certainty in the same way as Option B.

The inclusion of the aspects listed (Option B) provides certainty regarding the supervisory expectations and ensures that there are safeguards within institutions not covered by the CRD; this option also provides legal certainty and clarity regarding supervisory expectations for institutions subject to the CRD. This is desirable to achieve harmonisation, but also because of consumer protection aspects (e.g. the continuous functioning of payment services should be ensured).

Option B has been retained.

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

Documentation should be comprehensive, provide an appropriate overview on outsourcing arrangements (including the main risks identified regarding the outsourcing of critical and important functions) and allow for the identification of concentration risks on a micro level by institutions and payment institutions and on both a micro and a macro level by competent authorities.

Option A: requiring institutions and payment institutions to document all outsourcing arrangements, but without specifying further requirements.

Option B: requiring institutions and payment institutions to document all outsourcing arrangements and to maintain a register for all existing outsourcing arrangements.

Option B1: limiting the register to only the outsourcing of critical and important functions.

Option B2: having all outsourcing arrangements documented in the register, but with the extent of documentation that is required differing between critical or important functions and other outsourcing.

Option C: the same as Option B, but requiring that planned outsourcing arrangements also have to be documented in the register as soon as their implementation is likely.

Option D: in addition to requiring a register, requiring institutions and payment institutions to liaise with competent authorities regarding all new outsourcing arrangements of critical and important functions, but leaving the details to the competent authorities.

Option E: the same as Option D, but requiring prior approval or a non-objection procedure implemented by the competent authority.

Option A would not necessarily result in a comprehensive register that would be readily available for submission to the competent authority and would allow neither institutions nor their competent authorities to efficiently identify risk concentrations. A requirement to have a register of all cloud outsourcing arrangements already exists. Option A therefore has not been retained.

Option B would ensure that institutions, payment institutions and competent authorities have an overview of all relevant outsourcing arrangements and would be in a position to assess risk concentrations. By defining a minimum set of aspects to be documented, this option would ensure that there is sufficient information available to assess the risk posed by outsourcing, e.g. within the SREP. The information should be limited to reduce the burden. Additional information could always be requested by competent authorities.

Option B1 would lead to slightly lower costs, as not all outsourcing arrangements would need to be included in the register. However, documentation would be necessary in any case. By including at least a limited set of information (Option B2) for all other outsourcing arrangements, the identification of concentration risks would be even better than in Option B1. As a register would already exist, the costs would be low, as the costs would be limited to those involved in the input of a few additional data points into the register. Option B2 would be more efficient than Option B1.

Adding planned outsourcing to the register (Option C) would give competent authorities the possibility to evaluate the potential effect of upcoming outsourcing arrangements combined with other existing outsourcing arrangements. However, it would also lead to a situation where institutions and payment institutions would enter potential arrangements that would not come into effect, leading to minor additional costs for adding such arrangements to the register. However, if arrangements were entered into the register only if they were nearly certain, they would be entered relatively quickly and therefore this process might not ensure that competent authorities were informed in a timely manner about upcoming outsourcing arrangements.

Option D would ensure that competent authorities would be informed about upcoming outsourcing arrangements and would have the opportunity to intervene if they had concerns about potential risks or if such an arrangement would lead to a situation where the institution would become an empty shall that lacked the substance for ongoing authorisation. The impact on costs for institutions and payment institutions would be low, but if feedback from the competent authority (Option E) was expected, this might delay the implementation of arrangements and could therefore lead to additional costs. In most jurisdictions, such processes (Option D) already exist and therefore the costs would be limited to jurisdictions where no prior discussion had taken place. A dialogue between institutions and competent authorities regarding outsourcing improves the effective supervision of firms.

Options B2 and D have been retained.

6) Guidelines on the assessment of risks and the criticality or importance of outsourced functions and their continued monitoring

Option A: the guidelines would leave it up to institutions and payment institutions to develop their own assessment framework.

Option B: the guidelines would specify, in line with MiFID II and PSD2 requirements, the approach for assessing the criticality or importance of functions.

Option C: the guidelines would specify a framework for the ongoing monitoring of outsourcing 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 that there would be one harmonised framework that takes into account the assessment criteria provided in MiFID II and PSD2, but would provide additional criteria for the assessment of the impact of outsourcing arrangements. Assessing the operational risk impact is one aspect that is relevant for determining if an outsourced function is critical or important. Such risks include the so-called step-in risk that may be triggered if the service provider were in financial

distress and needed financial support by the institution or payment institution to maintain the services provided; this is particularly relevant for significant institutions. A harmonised set of criteria to be implemented by institutions and payment institutions would not create greater costs than if institutions defined their own framework. However, where there is already a framework in place that is in line with the MiFID II and PSD2 requirements, institutions would have one-off costs for adjusting that framework.

Option C would ensure that changes to the criticality or importance of outsourcing arrangements would be identified by all institutions and payment institutions. Under Option C, the guidelines would provide a more specific framework for monitoring outsourcing risks than the EBA Guidelines on internal governance, which are applicable to institutions subject to the CRD only. Option C would be effective. Additional costs would be limited to adjustments to the already existing risk management framework.

Options B and C have been retained.

7) Outsourcing of banking activities and payment services that require authorisation by a competent authority

Although most outsourcing arrangements involve activities or services (or parts thereof) that do not, in themselves, require authorisation by a competent authority, institutions may occasionally want to outsource functions or parts of banking or payment services or activities, to an extent that would require authorisation or registration in their Member State, to service providers located in third countries. The outsourcing of investment services is regulated under Commission Delegated Regulation (EU) 2017/565 of 25 April 2016.

The outsourced parts of banking activities or payment services may themselves require authorisation. However, the full service or activity, i.e. including the responsibility for the service or activity, can never be outsourced. While, within the EU, a common framework for authorisation and supervision applies, outsourcing to third countries would, in most cases, not be subject to the same framework. Therefore, this specific type of outsourcing arrangement should be allowed only if:

- the service provider in the third country is authorised by or registered at a relevant supervisory authority to perform the activity or service; and
- the outsourcing arrangement will not undermine the ability of the competent authority in the Member State to effectively supervise the outsourcing institution or payment institution. This will commonly require that the competent authority is able to receive the information needed for its supervisory tasks and exercise access and audit rights in the third country and that there exist mechanisms for the exchange of information on enforcement matters.

Two policy options have been considered.

Option A would allow the outsourcing of banking and payment activities or services, which are subject to authorisation or registration, to third countries only if there is an appropriate cooperation agreement between the competent authority of the institution and the supervisory authority of the service provider.

Option B would be an outcomes-focused approach and would require institutions and payment institutions to be satisfied that any proposed outsourcing of functions (or parts of banking or payment services or activities) that require direct authorisation to service providers located in third countries would not prevent or undermine the ability of competent authorities in their Member State to effectively supervise them. Competent authorities would have the power to take measures if effective supervision were not possible.

Option A would be in line with the approach for investment services under Article 32 of the Commissions Delegated Regulation, which requires such a cooperation agreement in the case of outsourcing functions of portfolio management; it ensures that the rights and responsibilities of the competent authority and the supervisory authority would be set out in writing.

However, such an approach would also require competent authorities to enter into multiple, lengthy negotiations with third countries to conclude the required cooperation agreements, even if institutions and payment institutions would need to be satisfied that there is a cooperation agreement between the competent authority of the institution or payment institution and the competent authority in the third country responsible for supervising such services or activities where they outsource those banking and payment activities or services. If a cooperation agreement does not exist, then outsourcing of banking and payment activities or services into the third country is not possible.

Option B recognises that effective supervision could be achieved through a variety of arrangements and mechanisms, including, but not necessarily limited to, cooperation agreements or supervisory colleges. Although more flexible and pragmatic, Option B would require competent authorities to determine that they can effectively discharge their supervisory duties in practice. In particular, competent authorities need to be satisfied that they will not be faced with restrictions regarding the exercise of information, access and audit rights. This is clearly more difficult without signing a cooperation agreement. Competent authorities would also need to reserve the right to require institutions and payment institutions to not enter into or terminate existing outsourcing agreements if the outsourcing concerned an activity or service that was itself subject to authorisation, if the competent authorities were not satisfied that they would be able to effectively supervise it. This approach would lead to legal uncertainty about the possibility of outsourcing functions to service providers in third countries.

Option A has been retained.

8) Setting minimum requirements for outsourcing contracts

To ensure that documentation requirements can be met, institutions and payment institutions need to have written arrangements in place that at least reflect the documentation requirements.

Option A: the guidelines would not set out additional contractual provisions above the aforementioned aspects.

Option B: the guidelines would define the minimum content of outsourcing arrangements, differentiating between critical or important outsourcing and other outsourcing. In particular, the guidelines would deal with the aspect of audit and access rights.

Option A would be in line with the principle of contractual freedom and the principle that the institution or payment institution is responsible for its outsourcing arrangements. Requirements specified in MiFID II and PSD2 would have to be met. However, such a guideline would not provide sufficient clarity regarding audit and access rights and other aspects that facilitate the appropriate management of outsourcing arrangements (e.g. termination and exit rights).

Option B would help institutions and payment institutions to agree on contracts that meet the minimum requirements expected by competent authorities, in particular with regard to the outsourcing of critical or important functions. The approach to audit, one aspect that is particularly difficult to negotiate, would be described in detail, leading to a higher level of efficiency at institutions and payment institutions when negotiating contracts. Such requirements are already included in the recommendation on outsourcing to cloud service providers and information and access rights are outlined in Article 65 CRD. The implementation of these requirements for other new outsourcing arrangements should not lead to additional material costs, in particular if the scope of such a requirement is restricted to a subset of outsourcing arrangements; instead it would ensure that outsourced activities can be monitored, audited and supervised.

Option B has been retained.

9) Guidelines for competent authorities

Competent authorities already supervise outsourcing arrangements under the SREP guidelines for institutions and as part of other supervisory processes for payment institutions.

Option A: the guidelines should provide a detailed procedural framework for supervision by competent authorities, including the timing of procedures and the need to assess new critical and important outsourcing arrangements before they are implemented.

Option B: the guidelines should ensure that competent authorities are appropriately informed of outsourcing arrangements, but would leave the setting of detailed supervisory procedures to the competent authority.

An assessment of outsourcing arrangements by competent authorities before their implementation (Option A) might lead to additional costs at institutions and payment institutions, as the implementation of processes could be delayed. Competent authorities would need to have additional staff resources to ensure a timely assessment.

Option B is sufficient, as the SREP is already harmonised within the EBA guidelines. For payment institutions, competent authorities are already informed about the outsourcing of payment services. However, given the periodicity of the SREP, additional information on new critical or important outsourcing arrangements, while carrying low additional costs, ensures that competent authorities can effectively supervise institutions and the concentration of outsourcing at service providers.

Option B has been retained.

E. Cost-benefit analysis

The guidelines impose a limited set of specific requirements on institutions, payment institutions and competent authorities under the already existing framework, providing clarification and procedural guidance.

A higher level of clarity on outsourcing requirements benefits institutions by creating a higher level of transparency regarding regulatory requirements and supervisory expectations. Standardised requirements lead to a reduction in costs for implementing processes, in particular when assessed on a consolidated basis.

Harmonisation should increase the efficiency of supervision. In particular, the identification and supervision of concentration risks by competent authorities may have a positive effect on the stability of the financial markets. However, this means that competent authorities will have to assign more resources to the supervision of such risk concentrations and/or may have one-off IT costs for establishing databases and inputting data to better track such concentrations. Those costs should be limited, as, on a risk-based approach, such measures should be limited to critical or important outsourcing.

The guidelines aim to ensure that institutions and payment institutions cannot become empty shells; this additional assurance protects the level playing field within the EU/EEA.

However, the guidelines will trigger some implementation costs for institutions (credit institutions and investment firms) and payment institutions, which will differ depending on their nature:

a. For payment institutions and investment firms subject to the CRD, considering that the sectoral directives already establish a set of requirements for outsourcing that is quite detailed, the additional costs should be very low.

b. For credit institutions subject to the CRD, a detailed framework exists regarding their investment and payment services and activities. Regarding banking activities, the previous CEBS guidelines form the basis of the EBA guidelines and therefore the additional costs triggered by the guidelines should be low overall.

For institutions and payment institutions, the guidelines may require an update of the current internal documentation, as well as the implementation and maintenance of a formal register in the form of a database. Some minor one-off costs may be triggered by the need to update outsourcing policies and to establish the register of all outsourcing arrangements (e.g. in terms of the additional data input on top of existing internal documentation). The overall impact is considered low, as institutions and payment institutions must already have documentation in place regarding their organisational structure, which includes outsourcing arrangements. Moreover, a formal register with minimum requirements will also be beneficial to the management of outsourcing arrangements and will improve the identification of risk concentrations on a micro and macro level.

The assessment of the criticality or importance of outsourcing arrangements by institutions subject to the CRD is also a requirement to consider. The criteria are consistent with other legislation in place; therefore, the additional costs are considered to be low. In addition, the guidelines provide clarity and harmonised criteria that need to be implemented by all institutions and payment institutions (i.e. not only by institutions subject to the CRD). The clear difference in the requirements for outsourcing critical or important functions and for other outsourcing arrangements benefit institutions and payment institutions in terms of the allocation of internal resources. The guidelines provide clear criteria to identify a function as critical or important, including where a defect or failure materially impairs the activities and financial performance. This is more evident for core business lines and critical functions already defined by the other legislation in place. Most institutions and payment institutions should have such processes in place regarding their investment and payment services and activities and, therefore, the roll out to banking activities should not be complex. The additional clarity, the protection of the level playing field and the proportionality of requirements all benefit the institutions and payment institutions. Therefore, the additional costs should be very low and should mainly be one-off costs for implementing the procedures needed. Given the existing procedures and the consistency with the other legislation that is already in place, the cost for applying new, more harmonised, procedures in the area of banking activities should be low. The risk assessment of outsourcing arrangements needs to include a more thorough assessment of the operational risks. The assessment of whether a function or part thereof is outsourced on a recurrent basis is a task already conducted on an ongoing basis. The identification of concentration risks caused by the outsourcing of multiple functions to one service provider may create additional, although low, costs, but only if this is not already part of the regular assessment of operational risk and concentration risk.

The guidelines provide clarification on the treatment of the outsourcing of functions by institutions and payment institutions when considered at the group level and when taking into account the possible interlinkages between operational risks. All institutions and payment institutions should already be familiar with risk assessments; all should already conduct scenario analyses at the individual and group levels and perform such risk assessments in line with other legislation and other EU guidelines, as they are obliged to manage all of their risks. Therefore, there are low additional costs for institutions and payment institutions.

Clear contractual requirements, including requirements to assure access and audit rights, lead to minor one-off costs and reduce the ongoing costs for negotiating outsourcing arrangements with service providers, as they establish a non-debateable set of contractual conditions to be agreed on. The clarification of supervisory expectations regarding outsourcing arrangements benefits institutions and payment institutions during the negotiations of contractual conditions and practical deliveries and creates a level playing field.

The specification of how audits can be performed regarding outsourcing is based on legislation and recommendations that are already in place and therefore does not trigger any additional costs; however, it does provide clarity about the supervisory expectations.

5.2 Feedback on the public consultation

1. The EBA conducted a consultation on the draft guidelines on outsourcing over a three-month period, ending on 24 September 2018; a public hearing was held on 4 September 2018. During the consultation period, the EBA, together with the chair of the EBA's Subgroup on Remuneration and Governance, had meetings with some significant European Associations (the European Banking Federation, the European Association of Co-operative Banks and the European Savings and Retail Banking Group) to discuss their concerns. Altogether, 59 responses were received, including the response of the EBA's Banking Stakeholder Group and nine responses that have not been published.

2. While many respondents acknowledged the efforts undertaken by the EBA to update the outsourcing guidelines and to integrate the EBA's recommendation on outsourcing to cloud service providers, several respondents made suggestions to reduce the scope of the guidelines and the regulatory burden that allegedly would be created by them. The main topics commented on are summarised below.

Main comments received during public consultation

Scope, definition and date of application

3. Respondents commented that the guidelines' scope of application and the definition of outsourcing were too wide. First, respondents required confirmation that the guidelines do not apply to subsidiaries that are themselves not subject to CRD on a solo basis, but only on a consolidated basis. In particular, the situation of alternative investment funds (AIFs), undertakings for collective investment in transferable securities (UCITS) and third-country subsidiaries should be clarified. Regarding the definition, many respondents provided examples of arrangements that should not be considered as outsourcing and requested the inclusion of a (non-exhaustive) list of arrangements that should not be considered as outsourcing in the guidelines.

4. Respondents also considered that the draft guidelines were too far-reaching, as they extend to arrangements that are not critical or important. They found it too burdensome that the risk assessment and due diligence provisions were in fact applicable to all third-party arrangements. Respondents suggested that the focus be only on the outsourcing of critical and important functions.

5. Respondents considered that the provisions regarding the transitional period were too restrictive. Respondents urged for existing contracts to be exempted from the scope of the new guidelines and for the end date of the transitional period to be postponed.

Proportionality and group application

6. Respondents found that the principle of proportionality had not sufficiently been taken into consideration and that the guidelines were in general too prescriptive. It was suggested that a more risk-based approach should be implemented.

7. Respondents felt that intragroup outsourcing, outsourcing within institutional protection schemes and cooperative networks, and the inherent lower level of operational risks due to the use of common service providers were not sufficiently considered; respondents suggested that lighter requirements be applied in relation to several matters (e.g. governance requirements, conflicts of interest, pre-outsourcing analysis, monitoring and audit requirements, exit rights, business continuity planning, documentation and notification, compliance and reporting obligations).

Contractual arrangements

8. Respondents found the contractual requirements too demanding and specific. They requested that a more principle-based approach be adopted and pointed out that certain expectations would raise significant legal and practical challenges, e.g. the inclusion of audit and access rights and the approach to sub-outsourcing that would trigger additional documentation and monitoring burdens.

Outsourcing to cloud service providers

9. Respondents suggested that the consideration of cloud services as outsourcing should follow the same principles as other services and technologies and determining whether they should be qualified as important or critical functions should depend on the nature of the activities outsourced. Other respondents would prefer to maintain the recommendation on outsourcing to cloud service providers.

Information to competent authorities

10. Regarding the information to be provided to competent authorities, respondents considered that the requirements were burdensome and sometimes had limited supervisory usefulness; this concerns the documentation of all, and not only critical and important, outsourcing arrangements and the need to notify competent authorities of new planned critical or important outsourcing arrangements. In addition, respondents highlighted that the requirement to inform competent authorities about outsourcing arrangements should be removed or converted into an *ex post* notification and requested confirmation that this is not to be seen as a prior authorisation procedure. Respondents also requested that the register of outsourcing arrangements be limited to critical or important functions.

The EBA's update of the guidelines

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

12. Overall, the guidelines have been reviewed to provide better differentiation between the requirements for the outsourcing of critical and important functions, to which a stricter framework applies, and for other, non-material, outsourcing.

13. The guidelines have been restructured to better mirror the MiFID II approach that (1) defines outsourcing, (2) defines critical and important functions and (3) sets out the requirements for institutions when outsourcing such functions. Considering the general governance requirements for institutions, the requirements for outsourcing of non-critical or non-important functions have been retained in a proportionate manner.

14. The guidelines have been checked for consistency with the EBA recommendation on outsourcing to cloud service providers and the PSD2 requirements on outsourcing.

15. It should be noted that, in general, all of the content of the recommendation on outsourcing to cloud service providers has been retained; however, changes to the approach have been made to ensure consistency with the overall outsourcing framework, which differentiates between the requirements for critical and important outsourcing and those for other, non-material, outsourcing arrangements.

16. The application of the requirements in the context of a group and an institutional protection scheme have been clarified. While the context of groups and institutional protection schemes needs to be taken into account, all institutions remain responsible for compliance with regulatory requirements.

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

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
General comments			
Subject matter, scope and definitions			
Mandate	Some respondents took the view that EBA alone does not have the mandate to set up rules that applied on a (sub-) consolidated basis, given that its mandate and expertise is restricted to banking business models. It has been proposed that cooperation be established between all European Supervisory Authorities to ensure a proportional approach to different businesses. One respondent commented that extending the CRD rules to subsidiaries that are subject to sector-specific rules, for which the EBA has no competence, is an infringement of the EBA's legal mandate.	Article 74 CRD requires that the EBA develop guidelines on governance; this includes developing guidelines on outsourcing. The guidelines take into account other relevant European legislation. There is close cooperation between all three European Supervisory Authorities. The guidelines are in line with Article 109 CRD, which requires that governance requirements be applied on a sub-consolidated and a consolidated basis.	No change
Regulatory changes	A few respondents suggested that upcoming regulatory changes (CRD V, CRR2, investment firms) should be taken into account.	The EBA can base its guidelines only on the current applicable EU legal framework. When new directives or regulations are adopted, the EBA will review its guidelines where necessary.	No change
Empty shell	One respondent asked for a more detailed explanation of when an institution is regarded as an 'empty shell'.	Please refer to the EBA opinion on issues related to the departure of the United Kingdom from the EU.	No change
Implementation across Member States	A few respondents asked for clarification on how the preferential treatment of intragroup structures is applied across different regulated jurisdictions (in and outside the EU).	In general, Member States should implement the specific requirements regarding the group application in line with Article 109 CRD. However, some Member States may impose	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		additional requirements, as the guidelines are subject to a comply or explain approach.	
Definitions	Some respondents requested that additional definitions be added to the guidelines that are already included in other directives or regulations (e.g. definitions of institution, credit institution, etc.)	The guidelines should not duplicate definitions that are already in force and included in Level-1 text (e. g. in the CRD, CRR or PSD).	No change
Prescriptiveness	Many respondents highlighted that the guidelines should maintain sufficient flexibility for EU institutions to react and adapt to market innovations and should not introduce burdensome requirements or restrictions, which could potentially reduce competition and/or increase the costs associated with the supply of services to institutions. Respondents suggested that the guidelines should differentiate between regulatory requirements (which are mandatory) and guidance (which allows flexible and proportionate application). Overall, it was suggested that the level of detail of the guidelines be reduced.	The principle of proportionality applies to the CRD, CRR and PSD and to all of the EBA guidelines. The guidelines provide further criteria for the application of this principle to ensure the consistent application of regulatory requirements. The guidelines specify the requirements set out under Level-1 text and therefore should clarify, with sufficient detail, how the requirements are to be applied in a consistent way. Please refer to the impact assessment included in this document.	No specific change; the guidelines have been clarified where appropriate
Cloud	Some respondents expressed concerns regarding the general assumption of the guidelines that every cloud solution is considered as critical or important, rather than each being examined on a case-by-case basis.	Cloud outsourcing follows the same assessment approach as other arrangements with service providers, taking into account cloud specificities.	The guidelines have been clarified
Brexit	Some respondents requested more flexibility, in particular due to Brexit and the potential increase of third-country service providers.	Please refer to the EBA opinion on issues related to the departure of the United Kingdom from the EU. The EBA is bound to apply and implement the applicable EU legislation, including with regard to third countries.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
GDPR	Some respondents suggested that the references to the GDPR be merged or reduced, or commented that the guidelines contained requirements related to data protection that were inconsistent or even conflicted with the GDPR.	The EBA assessed the guidelines before the consultation and did not identify areas that would contradict the GDPR.	The guidelines have been clarified
Oversight of service providers	A few respondents suggested that the EBA should work on a validation or certification framework for service providers, so that it would not be necessary for several institutions to perform individual assessments. One respondent asked for clarity over the role of the EBA and/or the relevant competent authority in the event of interruption of supply or supplier failure of a scheme provider or monopolistic supplier.	Competent authorities and the EBA have no direct role in the oversight of service providers that do not fall within the scope of their action. There is no legal basis for introducing a certification for 'approved service providers'. The responsibility for the selection of the provider lies with the institution. When service providers fail, and this failure leads to a material impact on the institution or the stability of the financial markets, competent authorities will take appropriate supervisory measures.	No change
Cooperation agreements between supervisory authorities	Respondents found the requirement that cooperation agreements (Memorandums of Understanding; MoUs) be signed in third countries too burdensome and a few suggested that other existing supervisory arrangements be considered that may facilitate cross-border supervision, including supervisory colleges and the idea that cooperation agreements may be informal. A few respondents recognised the need for Member State competent authorities to effectively supervise third-country outsourcing arrangements of regulated entities, but suggested that the home supervisory authority should maintain and issue a list of countries to which outsourcing is appropriate, rather than leaving the responsibility with institutions.	Cooperation agreements with authorities in third countries must be reliable and effective if functions are outsourced to an extent that would require authorisation or registration. Institutions need to be aware of such cooperation arrangements; therefore, only formal arrangements can be relied on. Competent authorities will be required to publish the existence of such arrangements. To ensure that existing outsourcing arrangements can be continued, the guidelines have been revised and transitional arrangements have been added. Where subsidiaries of EU institutions in a third country outsource functions to service providers in third countries to an extent that would require authorisation or registration,	The guidelines have been revised and clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	One respondent asked for confirmation that the requirement for cooperation agreements applies only in the case of outsourcing from an EU entity to a third-country entity, to avoid the need for cooperation agreements between supervisory authorities of two third-country subsidiaries of an EU parent institution.	cooperation agreements with the competent authority of the service provider are needed to ensure effective supervision on a consolidated basis.	
Mapping of requirements	Some respondents suggested that the specific requirements for each type of outsourcing (i.e. general outsourcing, outsourcing of a critical or important function, intragroup arrangements) be clarified and that the requirements for each type be compiled in a specific table or diagram.	The guidelines ensure that the scope of application of the requirements is sufficiently clear.	No change
Environmental, social and governance (ESG) standards	A few respondents suggested that the ESG standards to which service providers must adhere be left to the discretion of the outsourcing institution.	The guidelines refer to the code of conduct of the institution and to human rights; institutions need to comply with both, including if they have outsourced functions.	No change
Employee representation	A few respondents suggested that these guidelines should require there to be a process for consulting employee representatives and that institutions should perform an impact assessment on the effects on the employees and discuss it with the social partners.	Employee representation is set out under national laws. The CRD includes no mandate to harmonise the involvement of employee representatives.	No change
Consistency	Some respondents observed that the terms 'electronic money institutions' and 'e-money institutions' were not consistently used.	The consistency of and use of wording in the guidelines have been ensured.	The guidelines have been reviewed
Responses to questions in Consultation Paper EBA/CP/2018/11			
Question 1			

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
General comments on the scope and definitions	Some respondents supported the idea of aligning the definition of outsourcing with the one in MiFID II; others suggested different, narrower, definitions. Several respondents pointed out that the scope of the guidelines was wider than that of MiFID II, as the strict limitation to critical and important functions and the explicit exclusion of certain functions (e.g. advisory service, (personnel) training, billing, premises services and the purchase of standardised services) in MiFID II were missing from the guidelines. In addition, respondents noted that the EBA guidelines broadened the application by including 'parts thereof' in addition to the process, service or activity, as well as by addressing all outsourcing arrangements (i.e. also non-critical or non-important arrangements). Some respondents requested that, for the sake of clarity, these guidelines be limited in a proportionate and risk-based manner to 'critical or important' outsourcing arrangements. Several respondents commented that the legal basis for including non-critical and non-important outsourcing arrangements was not clear. The MiFID II framework limits the requirements to critical or important functions; establishing additional requirements for all outsourcing arrangements can be achieved at the legislative level only. The EBA therefore would, through these guidelines, go beyond its powers by creating new law.	The definition of outsourcing has been fully aligned with the definition in Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II. It would not be practical for institutions to apply different definitions for different activities (i.e. banking activities versus investment and payment services). It is the EBA's view that the definition applies also to parts of functions that are outsourced. Such parts of functions are themselves processes, services or activities that fall into the scope of the definition. The additional explanations have been moved into a different section to avoid any confusion with the definition of outsourcing. However, other non-material outsourcing arrangements should also be managed by institutions as part of their governance arrangements. Article 74 CRD includes a specific mandate for the EBA to develop guidelines on governance, including the operational structure of institutions. Outsourcing arrangements are part of institutions' operational structure. Similar governance requirements exist in the PSD2 and MiFID II. In addition, the EBA is mandated within Article 16 of its Founding Regulation (EU) 1093/2010 to provide guidelines within its scope of action. The EBA has reviewed the guidelines and introduced, taking into account the principle of proportionality, further simplifications for other (i.e. non-material) outsourcing arrangements.	The definition has been revised and the guidelines have been clarified
Application to specific firms (central counterparties (CCPs), central securities	Some respondents requested that a clarification be given regarding whether CCPs or CSDs holding a banking licence and MLTFs operated by investment firms would need to comply with the EBA guidelines over and above existing sector-specific	The guidelines set out how Articles 74 and 109 CRD and the requirements within the PSD2 are applied with regard to outsourcing functions. All institutions that are subject to those requirements are addressees of the guidelines.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
depositories (CSDs) and multilateral trading facilities (MLTFs)) and critical infrastructures	regulations. The respondents suggested that CCPs, CSDs and MLTFs be exempted from the scope of the guidelines, as otherwise this could lead to duplications or inconsistencies in the requirements. Other respondents suggested that the guidelines should apply to all service providers. Two respondents highlighted the specific position of financial market infrastructures (FMIs)/critical service providers (CSPs) and suggested that FMIs/CSPs should not be subject to the guidelines, as they are already adequately supervised or overseen by financial regulators.	The guidelines cannot be addressed to service providers that are not directly subject to the underlying regulatory requirement. As regards the question of whether the service provided by a CCP or being a member of a MLTF is considered outsourcing, the guidelines have been clarified and, in general, this is not the case. The same applies to the provision of market infrastructures, even if they are considered critical.	
Third-country application	A few respondents were concerned about the extraterritorial impact of the requirements and suggested that the competitive impact on entities located in, and outsourcing within, third-country jurisdictions be considered.	The guidelines cannot deviate from Article 109 CRD, which prescribes how requirements should be applied on a prudential consolidated basis, including in third countries.	No change
Definition Obligations to outsource	Some respondents stressed that services performed on the group level (e.g. a central unit) on a mandatory or optional basis should not be deemed as outsourcing. In some jurisdictions (e.g. Austria and Italy), the cooperative banks are required to outsource certain services or processes to the central body.	The central performance of a function on the group level may well fall within the definition of outsourcing. In all cases, the risks have to be managed. It has been clarified in the guidelines how the requirements should be applied in a group and in an institutional protection scheme context.	The guidelines have been amended and clarified
Definition Examples	Many respondents suggested that the non-exhaustive list of examples of arrangements that do not fall into the scope of outsourcing should be extended.	The detailed arrangement has to be taken into account when assessing if an arrangement is considered an outsourcing arrangement. However, a few additional examples that are in general considered as purchasing have been added.	Additional examples added

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Definition IT outsourcing	Particularly in the context of IT services, respondents commented that there are many services that, in a practical sense, would never be undertaken by an institution (e.g. as they have evolved recently, such as cloud services). Therefore, respondents suggested that, where an IT service is not critical for the provision of continuous and satisfactory service to clients, it should not fall under the term 'otherwise be undertaken by the institution' under the term 'outsourcing'.	Institutions need to take into account jointly all functions that are provided by a service provider when assessing if an arrangement falls under the definition of outsourcing (e.g. the provision of IT infrastructure together with data backup services). Even if such an arrangement would not be considered as an outsourcing arrangement, e.g. as it would simply be the procurement of hardware or storage space, institutions must manage the risks resulting from such a third-party arrangement.	The guidelines have been clarified
Cloud outsourcing	A respondent suggested that the guidelines be aligned more closely with the language of the EBA's recommendations on outsourcing to cloud service providers, so that institutions are assured that they can continue to follow the existing regime. Some respondents requested that the approach towards cloud outsourcing be reviewed and that a more proportionate approach be taken; in particular, a differentiation between material and non-material outsourcing was suggested.	The EBA in general retained the approach taken towards cloud outsourcing, but introduced a better differentiation between the requirements for critical and important outsourcing and non-material outsourcing, which also applied to cloud outsourcing arrangements. In a few areas (e.g. audit rights and documentation), further clarifications have been necessary to ensure a more uniform application in line with supervisory expectations and the general outsourcing framework.	The guidelines have been clarified
Payment and electronic money institutions	A few respondents urged the EBA to exclude payment and electronic money institutions from the scope of the guidelines (at least in their starting years) to promote start-ups. Two respondents suggested that these guidelines apply to payment and electronic money institutions only when they outsource an operational function, in particular providing that their service through an agent (distributor) is already sufficiently regulated.	The guidelines allow for a proportionate application of the requirements. The proportionality criteria provided in the guidelines do not form an exhaustive list and payment institutions may use additional criteria. In addition, start-ups that are payment institutions or electronic money institutions have to comply with the regulatory requirements that form the basis of the guidelines.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Other respondents requested that there be a more proportionate approach for payment and electronic money institutions than for institutions subject to the CRD. A few respondents highlighted that the PSD2 needs to be considered and specific chapters should be included to highlight the different requirements for the different types of institutions, which would be required to achieve a proportionate and risk-based approach and would be in line with recital 10 PSD2 and recital 4 EMD2.	The provisions within the guidelines already take into account the regulatory framework (PSD2/EMD2). Where necessary, the guidelines specify the requirements for specific types of firms. Due to the largely similar framework, it was not considered efficient to split the guidelines into a set of guidelines under the CRD and a set of guidelines under the PSD/EMD.	
Paragraph 5	A few respondents suggested that the scope of the guidelines be limited to critical/important outsourcing agreements, as otherwise financial institutions could be prevented from entering into a non-critical/non-important outsourcing agreement with a service provider unless a contractual right for the institution and its competent authorities to access and audit the service provider was granted. A few respondents suggested that the definition of 'critical and important' be supported by additional, relevant, non-exhaustive examples of services that fall outside the definition.	The guidelines have been reviewed, including the definition and criteria for assessing the criticality or importance of a function, and the supervisory expectations have clarified, better differentiating between the outsourcing of critical or important functions and other outsourcing arrangements.	The guidelines have been revised
Paragraph 9 Application on the solo level for firms within the scope of prudential consolidation	Several respondents noted that it should be explicitly stated that investment management companies, which are already authorised under the UCITS Directive or the Alternative Investment Fund Managers Directive (AIFMD), are not in the scope of application of the guidelines.	In accordance with Article 109 CRD IV, firms subject to the UCITS Directive or the AIFMD are in the scope of prudential consolidation and therefore are covered by the application of the guidelines on a consolidated level, but not on an individual level.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraphs 12 and 13	Nearly all of the respondents commented on the date of application and transitional arrangements and asked them to be postponed. Many also requested that the change of existing contracts not be required, as this would infringe the principle of legal certainty. Some respondents are concerned that they have to discontinue existing arrangements, as cooperation arrangements may not exist or cannot be negotiated. One respondent pointed out that EBA/REC/2017/03 requires that contracts are documented in the register only if they are new or renewed and urged the EBA to align the guidelines with this approach. One respondent considered that two distinct implementation timelines for cloud and other outsourced services would be costly to implement and suggested that the implementation time frames be harmonised.	The date of application has been changed to 30 September 2019 and the period for transitional arrangements has been prolonged. Where contracts have not been updated, additional supervisory scrutiny is needed to ensure that institutions have robust governance arrangements in place. In the case of outsourcing functions, which themselves require authorisation, to third countries, the requirement of cooperation agreements is needed to ensure that the institution can be effectively supervised, which is one requirement for the authorisation of institutions. Institutions need to document all outsourcing arrangements and have a register of outsourcing arrangements, as set out in the guidelines. A register of outsourcing arrangements is needed to ensure the effective supervision of institutions and to be able to identify concentrations at certain service providers. The register has been simplified for non-critical arrangements. The EBA recommendation on outsourcing to cloud service providers is already applicable, i.e. the time frame cannot be adjusted.	The guidelines have been clarified and transitional arrangements have been revised
Definition Critical or important function	Several respondents asked for clarification about whether the term 'critical or important' should be considered as one category or as two different levels of importance. Respondents requested a non-exhaustive (negative) list of non-critical and non-important functions (e.g. market communications). One respondent asked whether the term 'material' has been replaced entirely.	The definition of the wording 'critical or important' is the same as that used under MiFID II, namely it is one category of outsourcing arrangements. The term 'critical function' used in the BRRD is a different concept and has a different definition under the BRRD framework. The term 'material' used in previous CEBS guidelines have been replaced to ensure consistency with Level-1 requirements.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Respondents requested that the term 'critical function' be clarified, as it has a different meaning under various regulations (e.g. the BRRD).	Some examples of non-critical and non-important functions (i.e. non-material functions) have been added.	
Definition Critical or important	A few respondents suggested that any intragroup outsourcing within a national group or a group surprised by the single supervisory mechanism be expressly excluded from the definition of 'critical or important function', as these arrangements are less risky.	The importance of outsourcing arrangements has to be assessed based on the criteria provided in the guidelines for both intragroup outsourcing and outsourcing outside the group.	No change
Definition Critical or important	A few respondents requested that a reference to any operational task performed by the internal control functions be removed, as this would implicitly require that any internal control function tasks be considered as critical or important, which would not be true.	The comment has been accommodated; however, where outsourcing of parts of control functions happen, this should be considered as critical or important if it can impair the proper functioning of institutions' internal control framework.	The guidelines have been revised
Definition Sub-outsourcing	Some respondents requested further clarification regarding the definition of sub-outsourcing and suggested that sub-outsourcing be clarified as concerning only the service that was delegated and not the governance arrangements of the service provider or the infrastructures used by it. Some respondents suggested that any requirements regarding sub-service providers be deleted and that the institutions' responsibility be limited to their direct counterparties or at least that the requirements be limited to critical or important outsourcing arrangements. Other respondents requested that the definition be limited to services relevant for the outsourced function.	The definition has been clarified. A situations is also considered sub-outsourcing where parts of the outsourced function are provided by a sub-service provider. The assessment follows the same pattern as the assessment of institutions' arrangements with third parties. Sub-outsourcing can change the risk and reliability of outsourcing arrangements. Therefore, the institutions must have a say and be aware of such arrangements, in particular regarding critical or important outsourcing arrangements, while the initial service provider also has monitoring obligations. The institution remains fully responsible for the function and compliance with regulatory requirements in the case of outsourcing and sub-outsourcing.	The guidelines have been revised

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Some respondents proposed that the guidelines should clearly state where multi-level sub-outsourcing is allowed and where it is limited to one level of sub-outsourcing.	Sub-outsourcing along the chain of service providers is not limited, as long as the conditions of the guidelines and the contract between the institution and the service provider are met.	
Definition Service provider	One respondent asked for clarification regarding whether a branch is considered a service provider when providing a service to another branch within the institution.	Branches are non-independent parts of an institution and therefore services provided by a branch are not outsourcing.	No change
Definition Cloud	Respondents, while pointing out that cloud outsourcing and the types of it are defined terms, urged the EBA to take a more technologically neutral approach so that the guidelines would be capable of including new or emerging IT services. A few respondents suggested that a lighter framework be created for outsourcing to 'multi-tenant service providers'. One respondent highlighted the need to take into account that many cloud products are characterised by being highly standardised services, which are offered to a broad range of customers and undertaken by monopolists (e.g. Microsoft, Oracle and SAP). Therefore, respondents argued that it should be acknowledged, as in the BaFin's MaRisk, that multi-tenant service providers of standardised IT services cannot comply with all regulatory requirements and a proportionate approach should be allowed (in particular regarding access and audit rights and the required minimum content of contractual arrangements). Respondents also noted that the guidelines' requirements relating to cloud services are generally ICT specific and therefore should not be included in an outsourcing contract solely on the basis that some components are in a cloud environment.	The guidelines do not restrict or promote the outsourcing of certain IT structures or technologies. It was decided that the EBA recommendations on outsourcing to cloud service providers would be integrated into the general outsourcing framework. Institutions should comply with all regulatory requirements, including with regard to their outsourced functions, independent of the fact that they may be standardised or provided by monopolists. The named service providers are currently themselves not directly subject to the regulatory requirements set out in the CRD. The guidelines – in the same way as the cloud recommendation – already include simplifications, e.g. with regard to the performance of audits, that also apply to the outsourcing of functions to multi-tenant service providers. However, audit rights are a basis for effective oversight and supervision and so need to be ensured contractually for at least critical and important functions and on a risk-based approach, in particular as it is assumed that institutions will progressively use cloud and other IT solutions. The definition of cloud services does not state that all cloud services are also outsourcing arrangements. However, all risks of arrangements with third parties have to be managed.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Institutional protection schemes (IPSs)	A few respondents suggested that a definition of an IPS be included, e.g. by referring to Article 113(7) CRR.	The comment has been accommodated in a footnote.	The guideline has been revised
Question 2			
General comment	A few respondents requested that, throughout the guidelines, it should be spelled out how proportionality should be applied with regard to the specific provisions.	The principle of proportionality needs to be applied based on sound judgement and considering the list of non-exhaustive criteria referred to in the guidelines. Providing detailed requirements for each and every situation would lead to an overly complex, prescriptive and inflexible framework.	No change
Proportionality Paragraph 15	Respondents welcomed the presence of the proportionality principle but asked the EBA to provide more clarity on the reference to the principle of proportionality, as they deemed the reference to the EBA internal governance guidelines to be insufficient, as the proportionality criteria included in these guidelines did not consider the complexity or scope of outsourcing arrangements. Some respondents suggested that outsourcing requirements should not be applied, based on proportionality considerations, to intragroup outsourcing or outsourcing to monopolists.	In line with the CRD (e.g. recital 54 and Article 74), proportionality in the area of governance applies with regard to the nature, scale and complexity of the institution. The criteria set out in the EBA guidelines include the fact that the group structure should be taken into account. The guidelines on outsourcing further specify how the guidelines should be applied. Proportionality does not mean that requirements are not applied; instead it means that requirements are applied in a proportionate way. However, a differentiation between the requirements for critical or important functions and other functions has been made, where appropriate.	No change
Types of service providers	Some respondents highlighted that there should be a clear distinction between regulated and unregulated service providers, as this would be in line with the principles underlying financial regulation.	The outsourcing institution remains responsible for the outsourced functions, whether the service provider is supervised or not. This aspect will usually be relevant within the due diligence process.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraphs 17 and 21	Respondents pointed out that the current wording of the guidelines implies that the guidelines have an extraterritorial application; respondents suggested that there should be a restriction of the scope to the authorised entities located in the EU. Other respondents suggested that the scope of application be limited to subsidiaries that are themselves subject to the CRD. A few respondents asked for further guidance on how this principle should be applied to the different risk models of AIF managers and UCITS managers. Respondents highlighted the importance of taking into consideration group recovery and resolution frameworks and the implementation of a proper exchange of information between EU competent authorities and resolution authorities to establish proportionality (in particular regarding Section 9.2, concentration risk in paragraph 59 and Section 12).	See comments on Question 1, paragraph 9. In accordance with Article 109 CRD , the guidelines cannot deviate from those provisions. The guidelines apply to subsidiaries, including subsidiaries located in third countries that are not directly subject to the guidelines, but are covered by its requirements on a consolidated basis, i.e. considering that the parent and its subsidiary would form one single entity. The responsibility to implement the guidelines and to ensure compliance with the guidelines lies, in that situation, with the consolidating institution. The guidelines follow the approach set out within Articles 21 and 109 CRD. Therefore, they are applicable on a group level only, if the waivers have been granted. The CRD does not set out waivers in the area of internal governance or outsourcing for institutions that are affiliated to a central body. The guidelines set out how the provisions should be applied in this specific situation where a waiver has been granted under the CRD. The existence of recovery and resolution plans cannot lead to a waiver of requirements in a business-as-usual scenario. However, some elements of such plans, e.g. exit plans, may in some cases be sufficient for the purpose of the outsourcing guidelines.	The guidelines have been clarified
Paragraph 18	Some respondents claimed that this paragraph extends the scope of the guidelines beyond the intention of Article 109(2) CRD, as it requires a solo-level application of the guidelines and overwrites the sector-specific rules.	All requirements of the CRD and PSD2 apply to institutions subject to those directives on a solo basis. Firms subject to the AIFMD and UCITS Directive need to comply on a solo basis with their own sectorial requirements.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraphs 19 and 20 Groups and IPSs	Several respondents commented that the proposed requirements on documentation, due diligence, concentration risk and exit strategy would be less relevant or even irrelevant from an intragroup or IPS perspective. The guidelines should recognise that the management of intragroup outsourcing should be proportionate to the risks presented by these arrangements. There should also be lower compliance and reporting obligations in these cases than for third-party outsourcing agreements. Various respondents stressed the importance of acknowledging that institutions that are part of certain financial structures (i.e. groups, IPSs and networks) do have to transfer tasks due to legal, regulatory or operational reasons or circumstances; such arrangements should not be considered as outsourcing. This would be particularly true in the case of small cooperative banks, which are either affiliated to a central body/institution in accordance with Article 10 or 113(7) CRR or embedded in a network. In particular, respondents noted that the services of clearing houses (within the framework of payment transactions and securities settlement), risk models, liquidity management and internal auditing performed by the parent undertaking or central institution should not be considered as outsourcing. Some suggested that the guidelines should better take into account the benefits of intragroup outsourcing, the degree of integration reached within many banking groups and the complementary measures and controls already required by other financial regulations such as the BRRD. For example,	The guidelines are in line with the CRD provisions. They cannot introduce waivers that go beyond the Level-1 or -2 requirements. Institutions have to have robust governance arrangements in place on an individual basis. The management body of an institution always retains the final responsibility for the institution, including for the appropriate management of all risks. Intragroup outsourcing and IPS outsourcing can indeed be cost effective and efficient ways of receiving or sharing services. Intragroup/IPS outsourcing is not free from risks. While a higher level of control needs to be taken into account, intragroup outsourcing must also be subject to appropriate decision-making processes. In addition, intragroup/IPS arrangements must be documented; this is obvious with regard to recovery and resolution planning requirements and is needed to ensure that institutions can be sure that such arrangements enable them to provide the services continuously to their customers. Potential conflicts of interests must be identified and managed; it cannot be per se assumed that intragroup outsourcing is free from such conflicts. Business continuity plans must cover the whole group of institutions or institutions within an IPS and must also be implemented and tested (e.g. by being involved in the central testing of arrangements) by single institutions within the group or IPS. The draft guidelines already included several alleviations for intragroup and IPS outsourcing, and these have been further	The guidelines have been revised and clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	intragroup risk management, measurement, controls and internal governance should be recognised in the guidelines. Respondents also noted that the parent undertaking, as the superordinate entity, should implement risk management and control processes to ensure its responsibility for compliance with prudential requirements on a group level, which also eliminates conflicts of interest. Some respondents claimed that there is no need for a documented exit strategy for intragroup and IPS arrangements, as the plans and operational resilience measures cover the issues in such cases sufficiently.	clarified. In particular, the requirements on exit strategies have been revised.	
Paragraph 19 BRRD	Respondents urged the EBA to align the requirements with the provisions of the BRRD and highlighted that intragroup arrangements should not be subject to replacement tests for third-party outsourcing, but should be dealt with within the context of shared service agreements, global recovery and resolution plans. The guidelines should not ignore the requirements for resolution plans laid down in Section A of the Annex to the BRRD and the final regulatory technical standards on the content of these plans (e.g. Article 7 of the regulatory technical standards) and should recognise the approved plans. Respondents noted that competent authorities should coordinate with the relevant resolution authorities when applying these guidelines to avoid duplication of work and urged the EBA to implement cooperation and information sharing between competent authorities.	The guidelines have been clarified. Where such plans include sufficient exit strategies from outsourcing arrangements, it is not necessary to define additional strategies for this purpose. However, it needs to be clarified that the BRRD requirements are tailored for a specific purpose that deviates from a business-as-usual scenario. Institutions should also consider in their operational risk and business continuity management that a failure of an internal service provider may have a material impact on their business activities.	Section on exit strategies amended
Paragraph 19	Respondents pointed out that the strict application of the guidelines in a group context could lead to situations where a	Articles 74 and 109 CRD require that there are robust governance arrangements on the solo, sub-consolidated and	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Group audit rights	subsidiary obtains the right to audit or monitor its parent company. This would contradict the fact that the parent company has the duty of oversight over its affiliated entities.	consolidated levels. This includes the fact that service providers can be audited, even if the service is provided by the parent institution in the way of a joint audit or outsourcing arrangement. Audit functions can be outsourced and the guidelines set out a range of audit mechanisms that can be used.	
Paragraph 19 Group outsourcing	Respondents noted that the CEBS guidelines acknowledged that the level of influence reduced the overall risk of outsourcing and that the new guidelines should not lead to a discontinuity of intragroup arrangements, as this would cause a higher risk. In addition, respondents highlighted that outsourcing to the lead institution is a crucial part of the steering function in a group.	The guidelines on outsourcing do not intend to restrict intragroup outsourcing, but specify the requirements that need to be fulfilled if functions are outsourced, including within groups. Indeed, within a group, the consolidating institution is responsible for implementing group-wide robust governance arrangements. However, this does not replace the responsibilities of individual institutions.	No change
Paragraph 19(b) and (c)	Some respondents suggested that paragraph 19(b) should be clarified, as it could be interpreted that the group has to maintain individual registers for all institutions for the competent authorities. Some respondents suggested that IPSs should be mentioned in paragraph 19(b) (central keeping of the register) and 19(c) (central monitoring and audit functions) to ensure consistency with paragraph 46.	Maintaining a register is the responsibility of the institution. Paragraph 19 has been clarified: the register and operational tasks of monitoring and audit functions can also be provided centrally within a group or an IPS.	The guidelines have been amended
Paragraph 20(a)	Some respondents commented that the current advantages of intragroup outsourcing are removed by the guidelines due to the negation of the lower level of risk; they suggested that there was no need to retain adequate competence and sufficient skilled resources to ensure appropriate management and oversight of the outsourced tasks as long as the reporting and impact assessment were fulfilled.	The guidelines do not restrict intragroup outsourcing. If there is, in the specific case in question, a lower level of risk, this will be taken into account in the risk assessment, even if it is performed centrally. However, institutions and members of the management body are responsible for ensuring robust governance arrangements and managing all risks. Without retaining sufficient competence	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
		and resources, this responsibility cannot be executed. The responsibility cannot be delegated, as otherwise the condition of authorisation would no longer be fulfilled.	
Paragraph 20(b)	Some respondents suggested that consistent terms be used for the 'pre-outsourcing analysis' throughout the guidelines and that the wording in the paragraph on 'pre-outsourcing assessment' be changed accordingly.	The wording has been aligned throughout the guidelines.	The guidelines have been revised
Paragraph 21	Some respondents proposed that, for institutions organised in a financial network (within or outside an IPS), a similar centrally organised regime as for groups, where waivers have be granted, should be recognised. An IPS is required to prove that there is no current or foreseen material, practical or legal impediment to the immediate transfer of own funds or the repayment of liabilities from the counterparty to the institution. Furthermore, the IPS has to demonstrate that it has suitable and uniform stipulated systems in place to monitor and classify risks and the corresponding possibilities to take influence, providing a complete overview of the risk situations of all the individual members and the IPS as a whole.	See comments on paragraphs 19 and 20. The waiver included in Article 21 CRD and Article 109(1) CRD in conjunction with Article 7 CRR are subject to approval by competent authorities, i.e. groups can benefit only if they meet the conditions and the waiver has been granted by the competent authority. They do not apply to an IPS. The guidelines are in line with the CRD provisions, but cannot introduce waivers that go beyond the Level-1 or -2 requirements. Institutions, even if they are part of a financial network or IPS, have to have robust governance arrangements on an individual basis.	No change
Question 3			
General comments	While some respondents were content with the approach taken and appreciated that the institution can apply some judgement, others stated that they would prefer it if more guidance and clear examples were provided. Some respondents provided examples of arrangements that should always be considered or should never be considered as outsourcing arrangements.	The guidelines set out the principles and criteria to be applied by institutions when assessing arrangements with third parties. In most cases and within a concise document, it would not be possible to clearly define examples that, in each situation, would lead to the same assessment results. However, a few more obvious examples have been added.	The guidelines have been revised and clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 22 Criteria to identify outsourcing arrangements	Some respondents stressed that the scope of outsourcing arrangements is further expanded due to the provision stipulating that, for the determination of outsourcing, it does not matter whether the specific institution is or will be able to perform the function itself or not. In some structures, the central institution or specialised entity is set up with the purpose of performing standardised services for the affiliated institutions that would not be able to undertake those services by themselves (due to small banks' lack of ability to bear the costs or to reach the level of quality safeguarded by those specialised entities). By considering it irrelevant whether an institution has performed that function in the past or would be able to perform it by itself, the number of contracts falling within the scope would increase significantly. Some respondents highlighted the need to include an element of time (duration or continuing) in the definition of 'outsourcing'.	When a function is normally performed by institutions in general and is provided by a service provider, the arrangement should usually be qualified as outsourcing, even if the individual institution has not performed it itself or would also not be able to perform it. An element of time duration has been added to the guidelines: outsourcing arrangements should be recurrent or ongoing services.	The guidelines have been clarified
Paragraphs 22 and 23	Several respondents urged the EBA to include a clear distinction between purchasing and outsourcing, while taking future technological developments into account.	The guidelines, via the definition of outsourcing, provide a clear set of criteria that should be used to determine outsourcing arrangements. The criteria have been further specified. However, even if something is purchased, institutions are responsible for managing the risks that may result from this arrangement. This is independent from future developments.	The guidelines have been clarified
Paragraphs 22 and 23	Some respondents sought clarifications about whether the purchase of standardised/licensed software of services that support IT platforms (e.g. web hosting, distributed denial-of-	The guidelines have been amended to take into account the concept of non-recurrent activities. Purchases of goods	The guidelines have been amended

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	service (DDoS) systems, data back-up processes) are considered as outsourcing or purchasing. Furthermore, confirmation was requested of the fact that such agreements would not be considered as critical or important (e.g. the failure of a DDoS protection system causing the payment institution's website to break down). Some respondents considered that services that are performed by all entities and are usually obtained from third parties or are not related to a licensed core banking activity or risk management are not 'normally performed by an institution' (e.g. bookkeeping, tax advice and tax compliance services, statutory reporting/accounting, custody audits, human resources, payroll accounting, purchasing computers, infrastructure, tenant-like electricity or other connections). Supporting tasks such as administrative or technical functions, e.g. logistical support in the form of cleaning, catering and procurement of basic services or products, should also not be deemed as outsourcing.	(including software licences) are not considered as outsourcing arrangements. Additional examples of purchasing have been added. However, institutions have to manage all of their risks when entering into an arrangement with third parties, including the operational risk of inappropriate or failing IT systems (soft- and hardware), and have to take appropriate business continuity measures.	
Paragraph 24	Some respondents requested that paragraph 24 be deleted, as it would go beyond the scope of the guidelines (in particular for intragroup/IPS internal purchasing). The requirement to perform a risk assessment or due diligence (in accordance with Sections 9.3 and 9.4) for all third-party arrangements is excessive and cannot be mitigated solely by applying the principle of proportionality.	The approach is maintained, but a closer link to the internal governance guidelines has been made within the guidelines; the link with the application of the proportionality principle is also further stressed.	The guidelines have been clarified
Paragraph 24	A few respondents considered that service providers would no longer be able to perform parts of licenced tasks on behalf of institutions without obtaining a licence, which is required for many financial technologies that use 'white label banking' (i.e.	It is not always the case that part of a licensed activity would require a licence. Authorisation requirements are set out within the CRD and PSD2. Whenever one of the activities that requires licensing is	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	an outsourcing arrangement with an institution to deliver its services).	performed, authorisation or registration is required in line with the applicable national law.	
Paragraph 25	One respondent requested a clarification on the sufficient steps an institution should take to verify whether a service provider in a different Member State is required to be authorised or registered and whether it fulfils the requirements. A few respondents asked for confirmation that payment institutions may involve service providers in offering regulated services through a system of chain outsourcing that includes non-regulated entities. Some respondents suggested that intragroup outsourcing be excluded from paragraphs 25 and 26.	Whenever institutions outsource functions to an extent that requires authorisation or registration, the function can only be outsourced to a service provider that is authorised or registered or otherwise allowed to perform the function within a Member State. The wording has been clarified. Additional requirements apply if the service provider is located in a third country. Where functions do not require licensing, they can be provided by any suitable service provider. However, it must be ensured that the conditions of the institutions' authorisation are respected. This also holds true in the case of sub-outsourcing. Institutions have to include appropriate checks within their due diligence process to determine if the service provider has an authorisation or is registered. The same principle also applies with regard to outsourcing within the group.	The guidelines have been clarified
Paragraph 26	Respondents requested a clarification on who will assess and how institutions should assess if a service provider is 'sufficiently supervised' and what will be the consequence if such arrangements do not meet the supervisory expectations.	In the first place, it is the institution's responsibility to ensure compliance with all regulatory requirements. Competent authorities will take appropriate measures if needed, including if they cannot supervise institutions effectively.	No change
Paragraph 26	A few respondents pointed out that problems occur especially in situations where a service provider is located in another state (a Member State or third country), in particular with regard to data protection requirements and the exchange of information under cooperation agreements.	Data protection regulations have to be complied with. Cooperation agreements require that third-country authorities apply equivalent confidentiality and data protection requirements. The guidelines have been clarified with regard to the forms of supervisory cooperation agreements expected.	The guidelines have been clarified and amended

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	While respondents agreed on the fact that the home supervisors need to be able to supervise the outsourcing institution, those respondents complained that the guidelines restrict paragraph 26(b) only to a MoU. Some requested that existing arrangements between the authorities or the cases in which a service is outsourced but no MoU is yet in place be taken into account.	Transitional arrangements for the existence of cooperation agreements have been introduced. Cooperation agreements are required only for functions that are outsourced to an extent that would require authorisation or registration if the service provider were located within a Member State.	
Paragraph 26	Some respondents stressed that competent authorities should be required to publish on their website which cooperation agreements are in line with the requirements (paragraph 26(c)).	Competent authorities will be required to publish the existence of cooperation agreements (MoUs).	The guidelines have been amended
Paragraph 27	A few respondents commented that, if a function has not been performed by the institution in the past, it cannot meet the requirement of retaining the ability to reintegrate the function or transfer it to another provider within an appropriate time frame.	If a new activity is going to be performed via an outsourcing arrangement, the institution must be able to oversee the activity or to integrate, transfer or end it within an appropriate time frame. New activities, even if performed by service providers, are also relevant for the ongoing assessment of the suitability of members of the management body and key function holders. The wording has been clarified.	The guidelines have been clarified
Paragraph 28	A few respondents suggested that the management body involvement be kept at a high level, i.e. the management body would participate in the definition and approval of the high-level outsourcing policy and in the reporting of material risks.	The involvement of the management body is defined within the CRD and PSD2 and for institutions in the EBA Guidelines on internal governance. The guidelines on outsourcing are consistent with those requirements.	No change
Question 4			
General comments	Many respondents found the requirements on outsourcing policy to be too specific and suggested that more freedom be given to institutions for developing an outsourcing policy document.	The guidelines have been revised to focus more on the outsourcing of critical and important functions. However, institutions need to manage all outsourcing arrangements.	The guidelines have been revised

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	Some respondents suggested that the policy should focus more on the outsourcing of functions that are critical and important. Some respondents found the conflict of interest requirements (in particular in group situations) to be not sufficiently clear (e.g. 'material conflict'). A few respondents suggested that the economic aspect (e.g. cost-effectiveness, reduction of risks) be taken into account by including provisions regarding a cost-benefit analysis. One respondent requested a clarification on whether the term 'policy' refers to a physical document or to frameworks and standards (i.e. a broader definition).	Conflicts of interest (see also the EBA Guidelines on internal governance) need to be identified and managed. They can occur at different levels, e.g. group entities, business lines or economic interests of members of the management body or staff. Institutions should also take into account their business needs and the costs and benefits of outsourcing arrangements. However, the present guidelines focus on the prudential aspects of outsourcing arrangements. The term 'policy' is based on substance rather than form; it does not matter if there is one document or if overall appropriate policies are in place.	
Institutions as service providers	Some respondents highlighted that these guidelines do not address the specific case whereby the institution is the service provider and urged the EBA to provide guidance for it.	The guidelines deal with outsourcing by institutions. Institutions can also be service providers and, in this role, are required to comply with all regulatory and contractual obligations.	No change
Outsourcing policies for payment and electronic money institutions	One respondent noted that Articles 19 and 20 PSD2 and the EBA Guidelines on the security measures for operational and security risks of payment services under the PSD2 already provide sufficient requirements regarding payment and electronic money institutions.	The guidelines are in line with Articles 19 and 20 PSD2 and set out further guidance on the supervisory expectations of outsourcing arrangements.	No change
Paragraph 28	One respondent asked who is considered the responsible 'management body' (e.g. for resolving conflict of interests) in the case of multiple group members using the same intragroup service provider.	Each institution is responsible for the management of its outsourcing arrangements and conflicts of interest, even if some operational tasks are performed centrally. On a consolidated level, this responsibility is with the EU parent institution.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 28(e)	A few respondents commented that day-to-day management is, by definition, a senior management task and not the responsibility of the management body.	The comment has been accommodated.	The guidelines have been amended
Paragraph 30	Some respondents considered that establishing a new function or key function holder would involve significant effort and be a burden (in terms of cost and time) and suggested that, instead, this responsibility should be left to the institution. Some suggested deleting this requirement completely. Respondents requested that the principle of proportionality be applied and that a member of the management body (especially in smaller or non-credit institutions, e.g. payment institutions) be allowed to be the responsible person. Furthermore, respondents highlighted that outsourcing rules should be in line with institutions' three line of defence approach.	The guidelines require that at least one person should be responsible for managing outsourcing arrangements or for establishing a function. This will depend on the size of the institution and the number and materiality of outsourcing arrangements. It is not a requirement that this person does not have other functions, as long as those functions do not conflict with the person's role as 'outsourcing officer'. It is indeed possible to assign the responsibility to a member of the management body. Indeed, the management of outsourcing arrangements should follow the three lines of defence approach, including, first, monitoring by the business, control by the second line of defence and, third, the audit.	The guidelines have been clarified
Paragraph 31(c)	A few respondents requested that the term 'operational' and the examples in brackets be deleted due to their implication of limiting the outsourcing, e.g. for the risk control function to operational tasks and to group structures.	The term 'operational' is intended to clarify that the responsibility for that function cannot be outsourced. It is possible to outsource tasks of internal control functions under the conditions set out in the guidelines.	The guidelines have been clarified
Paragraph 32(e)	Respondents requested that the term 'fintech' be deleted as it is already included in the term 'ICT', unless there are specific risks (then clarification would be required).	'Fintech' is a commonly used term that is also used in other EBA products; it is included in the term 'ICT'.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 32(g)	Respondents pointed out that paragraph 32(g), in combination with paragraphs 89-91, requires that an alternative service provider or the ability to reintegrate a critical or important function is needed to ensure comprehensive, documented and sufficiently tested exit plans; however, it is not always possible to meet these provisions. In addition, for critical or important functions, an exit strategy should not be required. Respondents highlighted that, in general, the guidelines should provide more clarity on what an 'appropriate time frame' would be. One respondent requested clarification on whether the reference to 'going concern' relates to situations where a supplier fails.	While the requirements of exit strategies have been revised, institutions must be able to ensure the continuity of the business activities or at least be able to end activities if a service provider cannot be replaced, the service cannot be provided internally or the continuity of the function cannot be ensured otherwise. The EBA refrained from providing an exact time frame, as this will depend on the impact of a potential disruption and the complexity of the outsourcing arrangement. 'Going concern' was added to differentiate the situation from a resolution scenario, but has been deleted as this may still be relevant under resolution scenarios, where the continuity of services is desired.	The guidelines have been amended
Paragraph 32(h)	Respondents pointed out that compliance with the GDPR is already stipulated by the GDPR itself and is subject to supervision by data protection authorities.	References to the GDPR have been centralised in the document, but were retained in the document for the sake of clarity.	The guidelines have been amended
Paragraph 33	A few respondents suggested that the guidelines should be restricted to consolidated entities to which the statutory outsourcing provisions are applicable. One respondent asked whether the application of the guidelines on the sub-consolidated level and on a consolidated basis is restricted to licensed entities established in the EU and to whom the statutory outsourcing provisions apply.	The guidelines follow the approach under Article 109 CRD. Institutions need to ensure that policies are implemented on a consolidated basis (prudential scope of consolidation). This consequently means that group policies should also apply to subsidiaries that individually are not subject to the CRD, including institutions located in third countries.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 34(b)(v)	One respondent stressed that this requirement is burdensome if any minor conflict of interest with third parties has to be identified.	The policy should detail the approach towards the management of conflicts of interests, including their identification.	No change
Paragraph 34(c)(ii)	Some respondents considered that this requirement was too detailed for a policy noted that clarification is needed regarding the fact that changes should be communicated only where they will have a relevant impact on the outsourcing arrangement.	The policy should detail the approach towards any changes related to the relationship that may have an impact on the institution. The policy should be established, taking into account the proportionality principle.	No change
Paragraph 34(e)	Respondents asked for clarification on the limitation to critical or important outsourcing arrangements (at least for paragraph (i)) and on the required measures an institution should have in place to prepare for a possible exit (e.g. should an agreement with alternative providers already be in place?).	The guidelines have been revised to focus more on the outsourcing of critical or important functions. Indeed, the guidelines explicitly mention that the policy should differentiate between outsourced critical or important functions and other outsourcing arrangements.	The guidelines have been amended
Paragraph 34(e)	Respondents stressed that it would not be proportionate to require small savings and cooperative banks or subsidiaries within a group to implement exit strategies for critical or important functions such as IT systems. The service providers of such structures are often owned by the cooperative network or group.	See comments regarding the group/IPS context.	The guidelines have been amended
Paragraph 35	Respondents asked for there to be a clear distinction between the various types of outsourcing and their different treatments, otherwise there would not be any bases for a distinct approach in internal policies.	The guidelines have been revised to focus more on the outsourcing of critical or important functions. Indeed, the guidelines explicitly mention that the policy should differentiate between outsourced critical or important functions and other outsourcing arrangements.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 35(c)	Respondents stressed that an IPS's ownership structure might differ from that of a consolidated group, in accordance with Article 11 CRR; therefore, there should be a clarification that other entities affiliated with the corresponding financial network should be covered, as should outsourcing arrangements between the member institutions; more detail should also be given on the less restrictive provision regarding intra group/IPS/network outsourcing.	See comments regarding the group/IPS context.	The guidelines have been clarified
Paragraph 35(d)	Respondents suggested that a proportionate approach would exclude sub-service providers or would at least limit the requirements for critical or important functions or for cases where data are stored outside the EEA.	Sub-outsourcing has not been excluded, as it has an impact on risks and the monitoring of arrangements. The guidelines have been revised to focus more on the outsourcing of critical or important functions.	The guidelines have been clarified
Question 5			
General comments	Some respondents considered that Section 5 should be clarified with respect to intragroup/affiliate outsourcing arrangements and how competent authorities should supervise it. A few respondents considered that the section on the internal audit function should be applied by the institutions on a risk-based approach. Some respondents highlighted that service providers, in particular multi-tenant service providers, often refuse access to their internal control files and findings, regulatory reports or intrusion tests due to confidentiality reasons. One respondent stressed that the PSD2 framework did not require any specific conflict of interest requirements.	The guidelines have been clarified regarding the group/IPS context. The internal audit function, in line with the guidelines and the guidelines on internal governance, should be applied on a risk-based approach. Institutions must comply with all regulatory requirements, including with regard to their outsourced functions, independent of whether or not the service provider is operating in a multi-tenant environment. Audit rights are a basis for effective oversight and supervision and need to be ensured contractually, in particular for the outsourcing of critical or important functions.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	A few respondents pointed out that the guidelines would need to take into account the fact that institutions can also act as service providers. Therefore, the different natures of the counterparties needed to be taken into account and the EBA should allow a different approach.	The PSD2 requires payment institutions to have robust governance arrangements. Institutions remain fully responsible in the case of outsourcing and it does not really matter if the service provider is an institution or not: the same requirements apply. This aspect can be taken into account in the due diligence process.	
Paragraph 37	Some respondents stressed that the assessment of conflicts of interest should be limited to critical or important services and that there were no (or very limited) conflicts of interest in the context of intragroup arrangements.	Conflicts of interest (see also the EBA Guidelines on internal governance) need to be identified and managed. They can occur at different levels, e.g. group entities, business lines or because of other economic interests of members of the management body or staff.	The guidelines have been clarified
Paragraph 38	Some respondents asked for clarification of what is considered a 'material conflict of interest' and a 'sufficient level of objectivity' for the purpose of this paragraph. Some respondents stressed that, in the case of group/IPS/cooperative structures, the principle of 'arm's length' cannot apply, as the strategic decisions take into account all parties interests causing no negative influences for anyone.	See comments on paragraph 37. It is the responsibility of institutions to assess their materiality and decide on and implement, as appropriate, mitigating measures. Imposing arm's length conditions is one measure to avoid conflicts of interest, also considering possible recovery and resolution scenarios. However, synergies within groups or an IPS context may be considered.	The guidelines have been clarified
Paragraph 39	Several respondents suggested that the institution and the service provider do not have to provide different business continuity plans; e.g. in the case of outsourcing to a data centre, it should be sufficient that the service provider establishes a business continuity plan that would then also be accepted by the bank.	The institution remains responsible in the case of outsourcing for its continuous operation; it should have a business continuity plan and it should ensure that this plan can be effectively implemented.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 40	A few respondents sought clarification of the term 'severe business disruption'. One respondent asked for criteria to be given to assess 'disaster recovery' and asked for clarification on how this differs from a business continuity plan. Some respondents suggested that backup testing should be required only when it is appropriate, as some providers do not have backup facilities and instead store data on active servers. Therefore, it should be availability that is ensured, not the testing of backup facilities. A few respondents asked for clarification on the use of the term 'periodically' and suggested that periodical testing not be required, as the costs are very high.	This section has been clarified and amended to accommodate the comments and to refer to the guidelines on internal governance.	The guidelines have been clarified
Paragraph 41	Some respondents asked if it is necessary for institutions to already have a contract with another service provider on hold for all critical or important outsourced functions or if such a contract should be on hold only for the functions bearing extraordinarily high risks, or alternatively if a risk-based assessment with documented contingency plans would be sufficient. Some respondents asked for clarification regarding the application of a business continuity plan on chains of outsourcing and asked about a risk-based approach.	Business continuity plans should take into account the possibility that the quality of the provision of the outsourced critical or important function will deteriorate to an unacceptable level or fails. Such plans should also take into account the potential impact of the insolvency, or other failures, of service providers and, where relevant, political risks in the service provider's jurisdiction. The guidelines do not require institutions to already have contractual arrangements with alternative providers.	The guidelines have been clarified
Paragraph 42	Some respondents considered that the review of outsourced activities (including on-site visits) performed under audit rights should not be limited to the internal audit function but should be set on an instructional level, allowing specialised (second or third line of defence) functions (e.g. IT, legal, compliance, etc.),	The management of outsourcing arrangements should follow the three lines of defence approach, including monitoring by the business, control by the second line of defence and audit.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	outsourced specialists (e.g. third-party certifications, external auditors, etc.) or a combination of the above to undertake them on a risk-based approach. The third line of defence should, on a risk-based approach, visit critical or important service providers, ensuring in particular that the guidelines' provisions are met; this is currently the responsibility of a mix of all three lines of defence. Some respondents stressed that there should be a reference to pooled audits and third-party certificates in this section (with a reference to paragraphs 74 and 75) and that many service providers do have an internal audit function; therefore, it should be clarified that their assessment and outcomes may be used (in particular if the service provider is an institution). One respondent was of the view that payment and electronic money institutions should not be required to have an internal audit function.	The guidelines focus on the third line, as it is the one usually in charge of audit. This is independent of ongoing monitoring activities that are also required. The guidelines specify that the internal audit function should perform its tasks taking into account a risk-based approach. Even if service providers do have an internal audit function, institutions cannot exclusively rely on it on an ongoing basis, at least for critical or important functions. Institutions are the ones subject to the regulatory requirements (see the section on audit rights). Payment and electronic money institutions should have sound governance arrangements, taking into account the application of proportionality.	
Paragraph 43	Many respondents considered that full audit rights are necessary only in the case of critical or important outsourcing, as negotiating those rights in all contracts (especially with third-country suppliers) would be burdensome. Many respondents sought clarification on how audit rights may effectively be enforced if the contractual rights are denied by predominant providers. Therefore, it was suggested that standardised reports (e.g. ISAE 34.02) be accepted for meeting the requirements of paragraphs 43 and 74.	The guidelines have been amended to accommodate the comments. Audit rights are needed for at least critical or important functions, otherwise institutions would no longer have robust governance arrangements in place. See new Section 13.3 on audit and access rights. The guidelines have been revised to allow for a more principle-based and proportionate approach. Institutions should also refer to the EBA's internal governance guidelines.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 44(d)	Several respondents suggested that the specific reference to the service provider's risk appetite, risk management and control procedure in relation to the outsourced function be deleted. The risk appetite of a service provider will differ from that of an institution (or it will not have one).	The guidelines have been revised. Implementing outsourcing arrangements should be conducted in line with the risk management framework of the institution and its risk appetite and strategy. Internal audit should ensure correct implementation.	The guidelines have been revised
Question 6			
General comments	Some respondents asked whether or not the register could be sourced from various data components or if it has to be a stand-alone data repository. One respondent stressed that Annex X is far too detailed. Some respondents suggested that a centralised register for cooperative networks without an IPS should be allowed and that the guidelines should clearly mention that the maintenance of the register could be outsourced. Some respondents sought clarification regarding the purpose of the register and how the competent authorities will utilise the gathered information. A few respondents asked for guarantees to be included in the guidelines about any commercially confidential information that may be contained within the register, as very sensitive matters are covered. It was suggested that the register should be internal and access to it should be limited. Some respondents pointed out that it would be impossible to provide all of the information on a sub-outsourcing provider and that proportionality should be applied.	It does not matter whether the register is sourced from various data components or if it is a stand-alone data repository, as longs as the information can be provided timely to the competent authority on request. However, to make it more effective and to ease the process, one single repository or the submission of one file to the competent authority would be more practical. Annex X has been deleted. The possibility of having a centralised register within groups or cooperative networks/IPSs has been included in the guidelines. See comments on groups/IPSs. Confidentiality should be ensured by institutions. Competent authorities are subject to professional secrecy obligations. The information required for the register has been reduced and the focus is now more on the outsourcing of critical or important functions.	The guidelines have been revised

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 46	Most of the respondents asked for the register to be limited to critical or important outsourcing arrangements. In particular, respondents argued that the burden is very high for including unimportant peripheral and substitutable services, compared with their low-risk impact. In the case that all arrangements remain within the scope, some respondents suggested that the information regarding non-critical outsourcing arrangements be limited to a brief definition of the outsourced function and the name of the service provider.	The information to be provided in the register has been reduced for non-material outsourcing.	The guidelines have been revised
Paragraph 47(a)	A few respondents suggested that the meaning of 'prudential consolidation' be clarified.	Prudential consolidation means the application of the prudential rules set out in the CRD and CRR on a consolidated or sub-consolidated basis, in accordance with Part 1, Title 2, Chapter 2 of the CRR. Prudential consolidation includes all subsidiaries that are institutions or financial institutions, as defined in Article 4(3) and (26) CRR, respectively, and may also include ancillary service undertakings, as defined in Article 2(18) CRR, established in and outside the EU.	No change
Paragraph 47(b)	A few respondents stressed that providing the legal entity identifier or registration number, parent companies and address are not necessary. A few respondents suggested that paragraph (b)(vi) be deleted, as the data are already required under the GDPR.	The comment has partly been accommodated. The information is needed for the register for the purpose of prudential supervision, so no change has been made in that respect.	The guidelines have been revised
Paragraph 47(c)	Several respondents suggested that the reference to cloud outsourcing be deleted, as this is against the principle of technology neutrality and would result in unequal treatment between cloud solutions and other outsourcing. Therefore,	The approach to cloud outsourcing has been revised and, for this specific form of outsourcing, an assessment of the criticality or importance is required.	The guidelines have been revised

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	cloud outsourcing should be considered as critical or important if it is assessed as such in accordance with Section 9.1. Some respondents were of the view that the term 'at least' should be deleted to allow for proportionality. Some respondents pointed out that some information (e.g. costs) should not be mandatory, as they are available only on an aggregated basis.	The use of the term 'at least' allows there to be a minimum list of information that institutions should include in the register. This allows for a level playing field among institutions when they are establishing the register and fosters sufficiently supervisory convergence, while allowing institutions to add additional information for their own purposes. The costs should be available and the guidelines specify that they should only be an estimate.	
Paragraph 47(c)(i)	One respondent deemed that the summary of the risk analysis should not be included in the register, as this would already be documented in the assessment of the criticality of the function.	If the information is already covered by the summary of the criticality assessment documented in the register then institutions may refer to that information.	No change
Paragraph 47(c)(v)	Some respondents suggested that these data fields be deleted, as the audit schedule is part of the internal audit documentation.	This information should be mentioned in the register.	No change
Paragraph 47(c)(vi)	Some respondents highlighted that this should not apply in a group context and therefore the term 'where applicable' should be added.	This also applies in a group/IPS context and therefore the information on substitutability should be provided.	The guidelines have been clarified
Paragraph 47(c)(ix)	Some respondents asked for the word 'location' to be replaced by 'country or countries' due to the security risks of disclosing the location of the data centre.	The comment has been accommodated; however, if the competent authorities requires more detailed information, e.g. to prepare an audit, more detailed information needs to be provided.	The guidelines have been clarified
Question 7			
General comments	Several respondents stressed that there are too many criteria for the assessment of the criticality or importance of a function and that several of them are part of the risk assessment. A non-	The guidelines are consistent with the requirements set out in the existing regulation and outline the requirements with sufficient detail to ensure their application in a consistent way.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	exhaustive list of critical or important services should be provided. Some respondents suggested that it be clarified whether each outsourcing arrangement has to be assessed on the solo and group levels. As soon as an outsourcing arrangement is deemed to be critical or important on any level, it should be treated as such, at least at the level concerned.	The criticality should be assessed on an individual level regarding the institution making use of the arrangement. For institutions that are part of a group or make use of intragroup outsourcing arrangements, the impact of criticality should also be assessed on a consolidated basis in line with Article 109 CRD.	
Title IV – Outsourcing process Paragraph 48(f)	Some respondents suggested that the expectations with regard to the pre-outsourcing analysis be clarified when the service provider is part of the accounting consolidated group.	Institutions should consider whether the service provider is a subsidiary or a parent undertaking of the institution, is included in the scope of accounting consolidation or is a member of or owned by institutions that are members of an IPS and, if so, the extent to which the institution controls it or has the ability to influence its actions in line with Section 2 of the guidelines. This section has been clarified and part of it has been moved to the risk assessment section.	The guidelines have clarified
Paragraph 49(b)	Some respondents stressed that the draft guidelines deviate from the requirements laid down in MiFID II and Article 30 of Commission Delegated Regulation 2017/565, as they consider any (full or in part) outsourcing of internal control functions as critical or important, whereas the MiFID II framework allows for a case-by-case assessment.	The comment has been accommodated; however, where there is outsourcing of material parts of control functions that could impair their proper functioning, this should be considered as critical or important, as such functions are key elements of institutions' internal control framework.	The guidelines have been clarified
Paragraph 49(c)	One respondent proposed that a definition of 'banking and payment services' be included, as it is not clear which services are addressed.	A reference to Annex I of the CRD has been included.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 50	Some respondents proposed that the paragraph be removed because not all cases of the outsourcing of activities, processes or services (e.g. some minor support functions) should be considered as critical or important, even if they relate to core business lines and critical functions.	To limit the scope, the guidelines have been amended to further clarify that the outsourcing of functions directly connected to core business lines and critical functions should be considered as critical or important, unless the institution's assessment establishes that a failure to provide the outsourced function or inappropriate provision of the outsourced function would not have an adverse impact on the operational continuity of the core business line or critical function.	The guidelines have been clarified
Paragraph 51	Some respondents considered that paragraph 51 should be moved to Section 9.3, as this paragraph is about risk assessment. Several respondents highlighted that the list should not be exhaustive and that the interaction between paragraphs 49 and 51 should be clarified (both list similar criteria, but paragraph 49 includes classification as critical or important as mandatory). Several respondents pointed out that these criteria do not take into account the specificities of group structures. Some respondents considered that a clarification was needed on how these requirements interacted with paragraphs 49 and 50. It was assumed that these were additional conditions to those in the other paragraphs. However, it was proposed that they be merged. A few respondents considered that the meaning of the term 'conduct' in paragraph 51(b)(iii) should be clarified (as it could related to customers, capital markets or employees, or others).	The guidelines have been clarified in line with the Commission Delegated Regulation under MiFID II, which defines the notion of critical or important functions for the purpose of outsourcing. To ensure consistent application, the guidelines provide additional criteria for the assessment of whether a function is critical or important. See comment on groups/IPSs. Conduct risk is a subcategory of operational risk and indeed refers to the conduct of institutions, including towards customers.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 51(a)	Some respondents suggested that the wording 'directly linked' be changed to 'directly connected' to reduce the scope. One respondent suggested that additional criteria for payment and electronic money institutions not be included, as Article 19(2) PSD2 already provides sufficient criteria. In particular, the requirements of paragraph 51(b)(i) would not allow a proportionate approach.	The comment has been accommodated. Institutions, when assessing whether or not an outsourcing arrangement is critical or important, i.e. whether it concerns a critical or important function, should take into account the criteria, meaning that the application of the principle of proportionality is also considered.	The guidelines have been amended
Paragraph 51(e)	Some respondents pointed out that this criterion should not apply on a group level, because it would lead to a situation in which several small outsourcing arrangements that were all non-critical or non-important for each group member were considered on aggregated bases.	Institutions are required to manage their risks also on a consolidated basis. This criterion should be applied on both the individual and the group levels.	No change
Paragraph 51(g)	A few respondents suggested that it be clarified that the assessment of scalability should focus on unexpected changes to the contract, which may result in a significant risk increase in connection with the outsourcing arrangement.	The scalability is linked to the fact that an outsourcing agreement might become critical or important over time.	No change
Paragraph 52	A few respondents suggested that this paragraph be deleted because the paragraph 51 would already sufficiently address the required quantification; respondents also commented that substitutability is not a relevant factor for the assessment of criticality.	The guidelines have been clarified and this paragraph has been deleted. Further guidelines have been included in the section on exit strategies.	The guidelines have been amended
Question 8			

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
General comments	Many respondents asked for clarification on whether or not the due diligence process applies to all outsourcing arrangements or only to the critical or important arrangements. Some respondents highlighted that there is not always a need for a due diligence process, or at least not on an individual basis for all institutions. It was suggested that the competent authorities perform this task by supervising the service providers or issuing quality labels or certifications. Another suggestion was that the EBA issue certification schemes in line with the Commission Working Group on cloud security certification schemes. Some respondents pointed out that the due diligence process, or at least some criteria of it, would not be necessary for intragroup outsourcing, as it would be redundant when adequate governance was set up and would sometimes be dependent on the outsourcing arrangement itself, such as the service provider's business model, nature, scale, complexity and financial situation. Particularly in the case of an IPS or a cooperative network, it would simply be a formal process, as the centralised entities are set up for the main purpose of providing the specific services and therefore the ability, capacity, resources and organisational structure are tailored to the needs and features of the members. Therefore, in such cases, institutions should be exempted from the due diligence requirement.	Institutions and payment institutions should ensure in their selection and assessment process that the service provider is suitable. Therefore, for all outsourcing arrangements to service providers, a due diligence process is required. This process can in some cases, e.g. within a group or IPS, be quite simple and should be performed in any case on a risk-based approach, i.e. taking into account the criticality of the function. The due diligence section focuses on the outsourcing of functions that are critical or important. Institutions are and remain fully responsible for the outsourced function and for performing the due diligence process. It is not to the responsibility of competent authorities to perform the due diligence process, as they are not responsible for the supervision of service providers. At the group/IPS level, the due diligence process should be performed; however, it can be done centrally. See group/IPS section.	The guidelines have been amended and clarified
Paragraph 53	One respondent considered that institutions should also ensure that the service provider has appropriate and sufficient 'infrastructure, in particular software, systems, etc.'.	All this should be covered in the due diligence process, which refers to the appropriateness of IT resources.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraphs 54 and 55	A few respondents sought clarification on how the service provider's nature, scale and complexity provides information on its ability and suitability to perform the service and what to consider as its 'nature'.	The nature of a service provider (e.g. regulated or unregulated), its size and the type of services it provides can give useful and effective information on the risks that an institution may face.	No change
Paragraph 56	Some respondents pointed out that, despite the importance of the ESG factors, no agreed taxonomy exists and guidance on how to integrate them into outsourcing arrangements would be more appropriate than simply mandating specific standards that may not be suitable for the service to be provided each time.	The guidelines refer to the code of conduct of the institution and to human rights; institutions need to comply with both, even if they have outsourced functions. The framework for sustainable finance, including ESG factors, will be developed in more detail in the future.	No change
Question 9			
Section 9.3 General comments Paragraph 57	Some respondents commented that the risk assessment section could better differentiate between requirements for critical or important outsourcing arrangements and for non-critical arrangements. A few respondents felt that the risk assessment requirements were too demanding and not tailored to intragroup outsourcing arrangements. A few respondents highlighted that it could be difficult for institutions to perform the risk assessment of sub-outsourcing activities and suggested entities analyse their provider's sub-outsourcing policies to guarantee adequate control of their risks and service level agreements, instead of actually verifying full compliance by each sub-outsourced provider.	Institutions should assess the risk before entering into an outsourcing arrangement and, in particular, should assess the criticality of the function. A risk assessment is needed for all outsourcing arrangements, even if in some cases it might be trivial. At the group/IPS level, the risk assessment can be done centrally, but institutions remain responsible for the decision to enter into the outsourcing arrangement. See section on groups/IPSs. Sub-outsourcing, in particular of critical or important functions (or part of them), should be in the scope of the risk assessment.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 58	Several respondents considered that the requirement to perform and document scenario-based risk assessments is too prescriptive and not proportionate, as it applies to each outsourcing arrangement. They consider that adequate risk management is also possible without using scenarios of risk events, in particular for non-critical outsourcing arrangements. One respondent considered that payment and electronic money institutions should not apply this requirement for the sake of proportionality and because the PSD2 and the EBA Guidelines on IT security do not require the general application of a scenario-based approach to risk management. One respondent asked for clarification on whether the estimation of the increase or decrease in operational risk as a result of an outsourcing arrangement could be qualitative. One respondent asked for clarification on whether the assessment is expected only as part of the decision-making process before entering into an arrangement or if it should be undertaken periodically.	The comments have been taken into account and the supervisory expectations have been clarified. The risk assessment, in particular for payment institutions and small and non-complex institutions, can be qualitative. Scenario analysis is an appropriate tool to assess operational risks; sometimes the risk assessment may be trivial and, depending on the scope of the outsourcing arrangement, no formal scenario analysis may be needed. The risk assessment should be done before entering into an arrangement, but institutions should monitor and manage their risk on an ongoing basis, i.e. risk assessments are not a one-off requirement but are part of the continuous management of institutions' risks.	The guidelines have been clarified
Paragraph 59	One respondent considered that the assessments of concentration and step-in risks duplicate other regulatory requirements that already cover those risks, such as business continuity planning and recovery and resolution planning.	Those risks are relevant for the purpose of these guidelines.	No change
Paragraph 59	Several respondents commented that it is not easy for an institution to assess concentration risk from outsourcing arrangements to a dominant service provider, as an institution would not have access to the (confidential and commercial) information required to conduct the assessment. This type of	The concentration risk of the institution towards a service provider should be assessed by the institution in the light of all outsourcing arrangement towards that service provider.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	concentration risk assessment, i.e. at market level, should instead be the responsibility of competent authorities.	The register and the information to be provided in it should facilitate the assessment of concentrations at market level by competent authorities.	
Paragraph 60	Several respondents considered it difficult for institutions, in practice, to have access to the relevant information to conduct risk assessments of multiple sub-outsourcers. Institutions should be responsible only for the relationship with their direct provider, and service providers should be responsible for, or at least participate in, the risk assessments in the case of sub-outsourcing.	If part of a critical or important function has been outsourced to a sub-service provider, this means that the institution gave its consent and therefore has assessed that the relevant information could be provided and that sub-outsourcing does not unduly increase its operational risk.	No change
Paragraph 61(a) and (c)	Some respondents asked for clarification on the meaning of 'sensitivity measures' and 'oversight limitations'. One respondent suggested that the word 'sensitivity' be replaced with 'criticality'.	Institutions should take measures to protect data in the light of their sensitivity (i.e. if they are of a personal or confidential nature). Outsourcing arrangements should not impede institutions' ability to oversee functions and competent authorities' ability to exercise their supervisory task, i.e. their should not be oversight limitations.	The guidelines have been clarified
Paragraph 61(d)	Several respondents considered that this requirement was too prescriptive and would significantly increase legal costs and the time to market, without being necessary for the overall risk assessment.	Political risks are a factor of operational risks and should be taken into account	No change
Paragraph 61(d)(iii) and (e)	A few respondents argued that data protection issues should not be addressed by the EBA outsourcing guidelines, but should be left to the applicable general data protection rules.	Data protection issues are not addressed by the EBA. A reference to the GDPR is nevertheless necessary to highlight the applicable framework and clarify the supervisory expectations.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 61(e)	Some respondents considered that this requirement should be applicable only to IT outsourcing, as it is typically designed for services related to data centres. One respondent asked whether security measures should be set out and defined in the outsourcing agreement. One respondent suggested that, for payment and electronic money institutions, this sub-paragraph be replaced with a reference to the EBA's IT security guidelines.	This paragraph is obviously oriented towards IT; it does not need to be clarified further. If specific data protection measures are relevant, they should be mentioned in the agreement between the institution and the service provider. For payment and electronic money institutions, the EBA Guidelines on IT security measures should be read in conjunction with these guidelines.	No change
Question 10			
Section 10 General comments	Many respondents asked that the guidelines be shorter, less specific and more principle-based regarding the contractual requirements. The whole section should apply only to the outsourcing of critical and important functions. One respondent considered that frequent use of terms such as 'should include at the least', in areas that are relevant to contracts, could encourage laundry lists and gold plating approaches and may lead to unnecessary friction and uncertainty during contract negotiations/repapering.	The guidelines have been clarified and focus on the outsourcing of functions that are critical or important. However, written outsourcing arrangements are required for all forms of outsourcing. The guidelines require a minimum set of contractual requirements and leave room for institutions to add further contractual clauses as required.	The guidelines have been clarified
Paragraph 62	Some respondents asked for clarification on what can be considered a written agreement, in particular to avoid restricting electronic signatures and digital contracting. Making reference to the eIDAS Regulation would be useful to this end.	All forms that are considered as 'written forms' under national law (including electronic forms) can be considered as a written agreement. The guidelines cannot specify this further.	No change
Paragraph 63	A few respondents suggested that standard contractual clauses be provided for the supplier negotiation process. Otherwise, financial institutions may find difficulty negotiating the terms of	It is not to the responsibility of the EBA to define a standard contractual clause.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	the guidelines with some large suppliers, e.g. the exercise of unrestricted access rights.		
Paragraph 63(a)	One respondent considered that describing the outsourced function should not be required for standardised services such as cloud services where service descriptions are usually not included in contracts.	A clear description of the outsourced function should be provided.	No change
Paragraph 63(b)	Some respondents did not consider it necessary to include an end date in the contract, provided that termination provisions are included.	The comment has been accommodated.	The guidelines have been revised
Paragraph 63(e)	Several respondents viewed this requirement as burdensome and costly, as locations can change, especially for cloud-based service providers. One respondent considered that the requirement in paragraph 63(e) that the outsourcing agreement must include the 'location' where data will be kept presents serious security concerns in the context of cloud services, including exposing the infrastructure and data centre personnel to increased risk of attacks.	The possible locations (i.e. country or region) should be mentioned, as this has an impact on the risks. Institutions need the exact location of the service provision to be able to fulfil their regulatory obligations, including executing audit rights, where needed.	The guidelines have been clarified
Paragraph 63(h)	Several respondents viewed this requirement as too broad, especially as service providers will be reluctant to accept such a clause. A few respondents suggested that the term 'unrestricted right' be replaced by 'necessary, appropriate or effective right'.	The EBA considers that this requirement is fully in line with other regulatory requirements. The scope of arrangements for which such rights must exist has been further specified in Section 13.3.	The guidelines have been amended
Paragraph 64(b)	One respondent noted that it is not possible for each service to define quantitative and qualitative performance targets and	It should be possible to specify indicators or quantitative and qualitative performance targets regarding the agreed service level.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	suggested that the term 'as applicable' be added to the sentence.		
Paragraph 64(e)	One respondent considered it inappropriate to impose specific mandatory insurance requirements on the service provider, as usual insurance policies will be used.	It is not a mandatory requirement to impose insurance requirements, but, if certain insurance policies are required, this should be specified in the contract.	No change
Paragraph 64(h) and (i)	Some respondents considered that no specific clauses in relation to insolvency law should be included, as general national insolvency law provisions will prevail over contracts. The EBA guidelines cannot provide sufficient legal clarity and should only include a requirement to reasonably address the insolvency risk.	Ensuring access to data is part of the business continuity measures. The guidelines do not interfere with the insolvency regulation and proceedings.	No change
Section 10.1	Several respondents suggested that a more proportionate approach on sub-outsourcing be taken, as this would not necessarily create more risks. In addition, respondents considered that requiring a high level of control over sub-contractors would raise practical issues, in particular regarding payment and cloud services. It is indeed extremely difficult for an institution to control a cloud service provider's outsourcing chain due to its dynamic nature. Several respondents asked for confirmation on whether the whole sub-section applies only to the outsourcing of critical and important functions. A few respondents suggested that the service provider should be held liable for any activity performed by third parties and that financial institutions should be kept informed of any sub-outsourcing by the service provider and should be able to swiftly	The section on sub-outsourcing applies to critical and important functions that have been outsourced by institutions. If such functions or material parts of them are sub-outsourced, the additional requirements apply. However, institutions may impose similar requirements also for other outsourcing arrangements, e.g. if they assume that the sub-outsourcing would increase their risks materially. In any case, institutions remain fully responsible for complying with all regulatory requirements when outsourcing functions. The liability of the service provider is part of the contractual arrangements that should be agreed between the service provider and the institution.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	exit the outsourcing agreement without cost. In such cases, institutions should be allowed to relax sub-outsourcing controls.		
Paragraph 65(d)	Some respondents considered that the prior approval requirement would be extremely challenging to obtain, especially for cloud or standardised services. It should be clarified whether the approval is of a general nature or if the institution should grant its approval to each case of sub-outsourcing. One respondent suggested aligning the language with Article 28(2) GDPR, which uses the terms 'specific or general written authorisation' instead of 'approval', and 'processing of personal data' instead of 'sub-outsourcing data'.	The guidelines have been clarified: prior authorisation can be provided in general terms.	The guidelines have been clarified
Paragraph 65(e)	One respondent asked for the expression 'in particular where' to be removed from the sentence to align it with the cloud recommendations and to avoid creating conflicting interpretations. One respondent asked for clarification on whether the service provider must inform the institution in all cases of changes to sub-contractors and prior to the sub-outsourcing arrangement.	The paragraph is clear enough and specifies the obligations in terms of the information needed, which aim to ensure that institutions can monitor and manage the risks of outsourcing arrangements where sub-outsourcing is planned or changes will occur. The notification period to be set should allow the outsourcing institution and the payment institution to carry out a risk assessment of the proposed changes before the changes come into effect.	The guidelines have been clarified
Paragraph 65(g)	Several respondents considered that the right to object should only be optional, provided that the notification requirement and the right to terminate an agreement in the case of undue sub-outsourcing are ensured.	Institutions have the final responsibility for the function and need to be informed about sub-outsourcing of critical or important functions. Where sub-outsourcing occurs, in the absence of an approval or no objection (depending on what is agreed), institutions should be able to terminate the contract.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 66	Several respondents requested clarification on whether the sub-contractor is not and should not be directly engaged with the institution. If this is the case, the obligations of paragraph 66 should be undertaken by the direct service provider on behalf of the sub-contractor. Several respondents asked whether the requirements apply to direct sub-contractors or to the whole chain of sub-outsourcing. In the latter case, respondents consider that it would be difficult to achieve compliance when sub-contractors provide only small parts of services. The requirements should therefore be proportionate to the role fulfilled and activity performed.	The sub-contractor is not obliged to directly engage with the institution. Institutions and service providers can organise the internal relationships themselves. However, it must be ensured that all regulatory requirements are respected and, where necessary, audit rights are granted. The section on sub-outsourcing applies to the chain of sub-outsourcing providers.	The guidelines have been clarified
Paragraph 66(b)	Some respondents asked for clarification on whether the audit and access rights would concern only the elements of the outsourcing that the sub-contractor is actually performing.	The audit rights relate to what is relevant for the performed function.	No change
Paragraph 67	One respondent considered that there is an inconsistency between this paragraph and paragraph 65(g), as the latter states that institutions have the right to object to any intended sub-outsourcing, while the former states 'if such a right was agreed'. Some respondents considered that the outsourcing institution should not have to impose its policy on a service provider, as the latter should have its own policy.	These paragraphs should be read in conjunction and do not contradict each other.	No change
Paragraph 68	One respondent asked for clarification on what the appropriate security standards are and asked if this could be those agreed in the contract or if it must be internationally accepted standards.	It is the institution's responsibility to define what the appropriate security standards are; further guidelines will be provided separately on the expectation of IT security measures.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	One respondent asked for clarification on the meaning of 'relevant providers' and asked if this was synonymous with providers supplying critical or important functions.	The word 'relevant' means where necessary in the specific case. It is not related to the service provider.	
Paragraph 70	Some respondents asked for clarification on what is meant by sensitive data and a risk-based approach, in particular whether the latter concerns a risk-based approach to locate data centres or an approach based on country risk.	In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, institutions and payment institutions should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations. In this particular case, 'risk-based approach' means that the risks related to the location and storage of data should be considered and managed in the light of the nature of the data (i.e. personal, confidential, non-confidential, public, etc.).	No change
Paragraph 71	One respondent suggested that the language be aligned with the cloud recommendation, in particular regarding the fact that service providers should comply with requirements regarding the protection of data that are applicable to them and not with requirements applicable to institutions. One respondent considered that the guidelines should recognise service providers' confidentiality obligations to other clients, security concerns, competition issues (e.g. audits by competitors) and professional obligations.	The guidelines are addressed to institutions and not to service providers. The guidelines recognise multi-tenant environments. When performing audits in multi-client environments, care should be taken that risks to another client's environment (e.g. the impact on service levels, the availability of data, confidentiality aspects) are avoided or mitigated.	No change
Paragraph 72	Several respondents consider that access rights should be limited to what is relevant for the function provided and only be required for critical and important outsourcing arrangements.	The guidelines have been amended regarding the scope of functions for which unrestricted audit rights are required.	The guidelines have been amended

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 72(a)	Several respondents considered that making arrangements for physical access to (all) data centres is unattainable and irrelevant (as there is likely to be nothing to see or the data are split over multiple locations) and that the guidelines should instead focus on relevant system information. One respondent considered that the competent authority's access to information should be done via the outsourcing institution and that the authority should not have direct access.	Both institutions and competent authorities should have unrestricted audit and access rights. This section has been clarified and sets out the appropriate audit techniques. Competent authorities have, by law, information gathering and information rights, including at service providers in Member States.	The guidelines have been clarified
Paragraph 72(b)	One respondent considered that a service provider should have the right to object to an inspection based on conflicts or competition.	Audit rights for institutions and competent authorities should be ensured and should be effective. Where such rights cannot be enforced for critical and important functions, such functions cannot be outsourced.	The guidelines have been clarified
Paragraph 73	One respondent asked for clarification on whether the audit function of the service provider can also perform the audit if the service provider has a banking licence.	The guidelines have been clarified. However, institutions cannot rely over time solely on the audit reports received form the service provider with regard to critical or important functions.	The guidelines have been clarified
Paragraph 73	One respondent considered that providing complete access to financial information was not possible for publicly listed service providers that are subject to strict reporting and disclosure rules and that such a requirement could inappropriately include information relating to other customers of the service provider.	The guidelines do not refer to the points mentioned, but audit and access rights must exist for what is relevant in the context of the outsourcing arrangement.	No change
Paragraphs 74 and 75	A high number of respondents considered that, to keep the cost of auditing low, especially in groups and cooperative banks, the final sentence should be removed. Shared (pooled audit) auditing or third-party reports should be sufficient if they are reliable and delivered in a timely manner,	For the outsourcing of critical or important functions, institutions and payment institutions should assess whether third-party certifications and reports, as referred to in paragraph 90(b), are adequate and sufficient to comply with	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
	and institutions and payment institutions should be free to decide whether further action is needed.	their regulatory obligations and should not rely solely on these reports over time. This limitation does not refer to pooled or external audits commissioned by the institution.	
Paragraph 75(f)	Some respondents suggested that the requirement be deleted, as it is not contractually conceivable, especially in groups or networks.	Audits should also be performed in group or IPS contexts. See comments on groups/IPSs.	The guidelines have been clarified
Paragraph 76	Some respondents stated that payment and electronic money institutions are not subject to the CRD framework for SREP but have their own framework on IT security and thus should not be required to carry out security penetration testing.	This requirement refers only to institutions (i.e. institutions subject to the CRD), not to payment institutions, which by contrast should follow the framework applicable to them.	The guidelines have been clarified
Paragraph 77	Some respondents suggested that the final part of the sentence be deleted and that the provision be aligned with the cloud recommendations.	In severe events and in some cases that depend on the nature of the outsourced function (e.g. cash management services, money transportation), it would not be possible to notify service providers about audits well in advance.	The guidelines have been clarified
Paragraph 79	Some respondents asked for the guidelines to specify what could be considered 'alternative ways to provide a similar level of assurance'.	When performing audits in multi-client environments, care should be taken that risks to another client's environment (e.g. the impact on service levels, the availability of data, confidentiality aspects) are avoided or mitigated.	The guidelines have been clarified
Paragraph 80	One respondent considered that a single institution could ensure only its own auditor's skills, not those of the whole pool of auditors.	Institutions are responsible for performing appropriate audits; similar to the review of certifications, participating institutions can, for example, jointly or by the exchange of relevant information, validate the suitability of auditors.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Section 10.4	Some respondents asked for the guidelines to better take into account IPSs and cooperatives, where termination can happen only on the basis of coordinated democratic processes.	Even in the case of groups/IPSs, institutions should be able to terminate arrangements, e.g. in the case of a recovery or resolution scenario.	No change
Paragraph 81	Some respondents asked why the guidelines referenced national law when clarifying what is meant by cross-border outsourcing arrangements and asked if that law applies to the institution or to the service provider. Some respondents suggested that the governing law of the agreement be referred to instead. Some respondents considered that the guidelines should require that reasonable termination rights be included in the agreement, but should not specify termination events, as some expectations of the guidelines, such as termination rights in the case of a breach of contract or any weakness of IT security, are not in line with some national laws and would be unenforceable.	The guidelines have been revised and now make reference to the applicable law, i.e. this may include national law, governing law and provisions with extraterritorial effect that have been included in the contract. The guidelines provide a list of non-exhaustive situations that may lead to the termination of contracts, based on the contractual arrangement. If institutions cannot enforce contracts, and this leads to their non-compliance with regulatory requirements, institutions must take appropriate action.	The guidelines have been clarified
Paragraph 81(b)	Some respondents considered that this provision is difficult to obtain from service providers and proposed that this sentence be deleted.	Where events happen that impede the performance of the service, institutions should be able to terminate the agreement, as, due to the inappropriateness of the service, the service provider may need to be substituted.	No change
Paragraph 81(c)	One respondent asked for clarification on whether the sub-outsourcing arrangements mentioned were only those related to critical and important functions.	The sub-outsourcing arrangements mentioned are only those related to critical and important functions. This paragraph should be read in conjunction with the section on sub-outsourcing.	No change
Question 11			

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Section 11 General comments	Some respondents stated that it would be challenging to monitor arrangements and performance on a continuous basis. Some respondents considered that the requirements of the section should apply only to outsourcing arrangements of critical and important functions.	The guidelines have been clarified. While institutions must monitor their outsourcing arrangements, the focus should be on the outsourcing of critical or important functions. Monitoring arrangements with third parties in general should be done on an ongoing basis and through a risk-based approach. See also comments below.	The guidelines have been clarified
Paragraph 83	Some respondents asked whether a central monitoring body must be established or if it is sufficient that the monitoring is performed by the institution's area receiving the service. One respondent suggested that the word 'ongoing' be replaced with the word 'regular' and another respondent suggested that a risk-based approach be referred to, especially for chain outsourcing.	The three lines of defence model should be applied for the management, control and auditing of outsourcing arrangements. Monitoring should be done on a risk-based approach. The word 'ongoing' stresses the fact that this is not a 'one-off' exercise and the interval of monitoring activities should consider the risks and can range from daily monitoring activities to longer intervals.	The guidelines have been clarified
Paragraph 85	Several respondents requested a clarification on the expected frequency of updates to the risk assessment. One respondent suggested that the term 'any risk' be replaced with 'material risk' and added that reporting should be done pursuant to the internal risk reporting governance framework. Some respondents asked about the extent to which the reporting can be delegated to committees.	The frequency is to be set by the institution and will take into account the monitoring results and the criticality of the function. The comment has been accommodated: the management body should regularly receive risk reports regarding critical or important functions. Board committees (i.e. risk committees) may assist the management body in its tasks, but the responsibility lies with the management body.	The guidelines have been clarified
Paragraph 88	Some respondents wanted the guidelines to specify the expected character of key performance indicators and key control indicators.	It is the institution's responsibility to define suitable indicators for the monitoring of the specific outsourcing arrangement.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Question 12			
Section 12 General comments	Some respondents asked that it be ensured that the requirements in this section were consistent with the BRRD. Several respondents considered that the whole section should apply only to outsourcing arrangements of critical and important functions. Some respondents considered that exit strategies should be required only when the continuity of services is endangered. A high number of respondents thought that the requirements of this section should apply only at the group/network level and/or to the central institution in cooperatives and IPSs. Only a pooled exit strategy should be required. In addition, respondents suggested that specificities of intragroup outsourcing arrangements be better reflected: since the likelihood that a service provider inside the group will be terminated or will fail is extremely low, greater visibility and cooperation is available and adjustments to intragroup arrangements are covered by business continuity plans. An institution may also not be in a position to exit an arrangement if this would conflict with the group policy or governance.	The EBA reviewed the guidelines and concluded that they are consistent with the BRRD. The guidelines focus more on the outsourcing of important or critical functions. The comment has been accommodated. The guidelines provide a list of situations in which exit strategies should be implemented. See comment on groups/IPSs. An exit strategy can be defined centrally.	The guidelines have been clarified
Paragraph 90	Several respondents were concerned that the term 'tested' could be misinterpreted, resulting in a successful transfer or in-housing of outsourced functions being requested, which would in fact be very burdensome.	The comment has been accommodated and 'where appropriate' has been added; in addition, it was clarified that the actual exit does not need to be tested in terms of a switch to another provider.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 90(a)	One respondent asked the EBA to confirm that institutions are not required to have in place alternative providers.	The guidelines specify that alternative solutions should be identified, but that no requirement exists to have alternate arrangements in place.	No change
Paragraph 90(b)	One respondent asked whether the scenario of a change in service provider needs to be included in the business continuity plan.	The change of service providers may be part of a business continuity plan.	No change
Paragraph 91(e)	One respondent considered that unacceptable service levels that can trigger an exit cannot be determined *ex ante* in a contract. They should also not be considered as the only cases in which exit from the arrangement may occur.	The institution can define *ex ante* performance indicators. See also comments regarding the ongoing monitoring of outsourcing arrangements.	No change
Question 13			
Section 13 General comments	Some respondents considered that there should not be additional new reporting requirements for payment and electronic money institutions. Such institutions are already subject to the PSD2 notification requirements and should not be required to have a register. Several respondents considered that intragroup outsourcing arrangements should be excluded from the information requirements. In particular, in IPSs or cooperatives in which a high number of affiliated institutions outsource the same function, providing the same set of information does not have added value.	The guidelines specify that payment and electronic money institutions already need to document all outsourcing arrangements. The register should be made available on request. See comment on groups/IPSs. A centralised register can be kept.	The guidelines have been clarified

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Paragraph 92	Some respondents considered that making a full register available within each SREP or at least every three years represents a significant volume of information that does not allow for risk-sensitive supervision. A high number of respondents made the following suggestions: that transmission be limited when supervisors request an inspection, that a waiver be provided for small institutions, that the scope of the register be reduced to critical and important functions and that the information required be limited (i.e. a brief description of the function, its criticality, contact details of the provider), with competent authorities then able to ask for more details when necessary. Several respondents asked for confirmation that no prior approval by the competent authority is necessary for an outsourcing arrangement. The requirement to inform competent authorities about outsourcing arrangements should be removed or at least changed to an *ex post* notification.	The register should be available upon request. The contents of the register have been streamlined, in particular for non-material outsourcing arrangements. See also comments on the register and in Section 11 on documentation. The guidelines do neither require nor prevent competent authorities from applying a prior approval process for outsourcing arrangements. Supervision is done on a risk-based approach and, depending on the size and complexity of institutions, a different frequency for reviews is applied. Institutions and payment institutions should adequately inform competent authorities in a timely manner or engage in a supervisory dialogue with regard to planned outsourcing of critical or important functions and/or where an outsourced function has become critical or important.	The guidelines have been clarified
Paragraph 94	Some respondents requested that this requirement be deleted, since the register would be sufficient.	See comments on paragraph 92.	The guidelines have been clarified
Paragraph 95	Some respondents asked for a clarification on the meaning of 'undue delay' and of 'material changes and events'.	See comments on paragraph 92.	The guidelines have been clarified
Question 14			

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Title V General comments	One respondent considered that this section should be integrated into the EBA SREP guidelines. One respondent wanted to add that competent and resolution authorities, and digital service providers' supervisory authorities, should cooperate for the monitoring of outsourcing risks.	These guidelines should be read in conjunction with the SREP guidelines. These guidelines are addressed to competent authorities. However, references and links to the BRRD framework are given where relevant. In particular, where risk concentrations are identified that pose risks to the stability of the financial market, the resolution authority should be informed about the new potential critical function (i.e. 'critical function' as defined under the BRRD).	No change
Paragraph 103	Several respondents asked that the specificities of intragroup outsourcing arrangements be better take into account, e.g. for the assessment of concentration risk.	Concentration risks within an institution, including on a consolidated basis, caused by multiple outsourcing arrangements with a single service provider, closely connected service providers or multiple outsourcing arrangements within the same business area should be considered and assessed on a macro level by the competent authority.	No change
Paragraph 104	Several respondents asked for a clarification on if and how competent authorities would inform entities about their calculation of concentration risk at a sector level, and what the consequences would be of evidence of a concentration risk, e.g. in the provision of cloud-based outsourced services.	Competent authorities should maintain a dialogue with the supervised entities. However, the concentration risk is assessed by competent authorities to identify risks for the financial stability; no public communication is required.	No change
Paragraph 105	Some respondents asked the EBA to better describe the situations in which a competent authority could ask an institution to exit from an arrangement to limit the business risk. The requirement to exit should be a last resort and prior steps and warnings should be defined as part of a supervisor's policy and made public by competent authorities.	No further clarification can be provided. The measures of competent authorities need to take into account in the situation in question. General principles of administrative law apply. This does not need to be specified in EBA guidelines.	No change

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Question 15			
Annex 1	Several respondents asked for clarification on whether the template provided was only an example; respondents asked if the EBA would explicitly allow institutions to have a different structure, template or application as long as it contained the required information.	The template was not intended to be mandatory and has been deleted.	The guidelines have been amended
Question 16			
Impact assessment General comments	Some respondents considered that the impact assessment failed to demonstrate that the benefits outweighed the costs. The latter are underestimated, as the guidelines will trigger significant financial, IT and administrative costs and an increased workload in terms of updating contracts, processes and procedures and performing on-going controls. Specific one-off costs identified include the design and set up of a database, the analysis of all contracts and the drafting of new clauses. Some respondents considered that the assessment underestimates the resources that will be necessary to maintain the register for all arrangements and for competent authorities to process the registers.	The impact assessment has been updated, taking into account changes made to the guidelines. The impact assessed reflects only the costs triggered by the guidelines and not the costs triggered by other regulatory products that already exist.	The guidelines and the impact assessment have been updated
Risk assessment	Some respondents considered that extending the risk assessment requirements to all third-party arrangements would have a significant economic impact.	This should not have a significant financial impact, as institutions are already obliged to identify, manage and monitor all of their risks. No sufficiently detailed information was provided by respondents to demonstrate the additional costs triggered specifically by the guidelines.	The guidelines and the impact assessment have been updated

Comments	Summary of responses received	The EBA's analysis	Amendments to the proposals
Cooperation agreements	One respondent found it difficult to understand the choice of Option A when the assessment acknowledged the length of negotiations for cooperation agreements and the impact of this on institutions' policies and practices.	The guidelines have been amended to allow for other forms of cooperation.	The guidelines and the impact assessment have been updated