Bitkom Position

Bitkom Position on EBA Draft Guidelines on Outsourcing arrangements

24 September 2018

bitkom

Bitkom
Federal Association for Information Technology, Telecommunications and New Media
Albrechtstraße 10
10117 Berlin
Tel.: +49 30 27576-0
bitkom@bitkom.org
www.bitkom.org

Contact person:
Julian Grigo
Head of FinTechs & Digital Banking
+49 30 27576-126
j.grigo@bitkom.org

Responsible working group: Digitaler Zahlungsverkehr (Digital payments)

Bitkom represents more than 2,600 companies of the digital economy, including 1,800 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 400 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.

Bitkom's members include over 40 FinTechs, over 15 banks and over 80 companies that offer software or infrastructure services for the banking sector, e.g. cloud service providers. The represented FinTechs offer their services across the breadth of financial services in areas such as P2P payments and investments, lending, wealth management, factoring, API banking, identity solutions, multibanking and platform banking.

EBA/CP/2018/11

22/06/2018

Consultation Paper

EBA Draft Guidelines on Outsourcing arrangements

Contents

Responding to this consultation

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

Comments are most helpful if they:

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

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 24.09.2018. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

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

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

Executive Summary

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

Over recent years, there has been an increasing interest of financial institutions to outsource business activities in order to reduce costs and improve their flexibility and efficiency. In a context of digitalisation and increasing importance of new financial technology (fintech) providers, financial institutions are adapting their business models to embrace such technologies. Some have increased the use of fintech solutions and have launched respective projects to improve their cost efficiency as the intermediation margins from the traditional banking business model are 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 (CRD) strengthens the governance requirements for institutions and its Article 74 (3) mandates the EBA to develop Guidelines on their governance arrangements. Outsourcing is one of the specific aspects of institutions governance arrangements. Directive 2014/65 (MiFID) and Directive 2015/2366/EU (PSD2) contain explicit provisions regarding outsourcing by investment firms and payment institutions.

The EBA is updating the CEBS guidelines on outsourcing issued in 2006 that applied only to credit institutions, in order to establish a more harmonised framework for all financial institutions that are within the scope of EBA's mandate, namely credit institutions and investment firms subject to CRD, payment and electronic money institutions. The guidelines set out specific provisions for these financial institutions' governance framework with regard to their outsourcing arrangements and the respective supervisory expectations and processes. The recommendation on outsourcing to cloud service providers, published in December 2017, has been integrated in the guidelines.

The financial institution's management body remains responsible at all times; to this end the management body should ensure that sufficient resources are available that appropriately support and ensure the performance of those responsibilities, including to oversee the risks and to manage the outsourcing arrangements. Outsourcing must not lead to a situation where an institution becomes a so called "empty shell" that lacks the substance to remain authorised.

Kommentar [MTU1]: Bitkom Comments: The topic of „Empty Shell" is addressed mainly in the foreword (e.g. under „Background" No 6). Bitkom would favour a more detailed explanation of when an institute must be regarded as an „Empty Shell".

With regard to outsourcing to services providers located in third countries, financial institutions must take particular care that compliance with EU legislations and regulatory requirements (e.g. professional secrecy, access to information and data, protection of personal data) are ensured and that the competent authority is able to effectively supervise financial institutions, including, in particular the critical or important functions outsourced to service providers.

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

Competent authorities are required to effectively supervise financial institutions' outsourcing arrangements, including the identification and monitoring of risk concentration at single service providers and to assess whether or not these could pose a risk to the stability of the financial system. To identify such risk concentration, competent authorities should be able to rely on a comprehensive documentation of outsourcing arrangements of financial institutions.

Next steps

The EBA will finalise these guidelines subsequent to the public consultation. The 2006 guidelines on outsourcing will be repealed after the EBA guidelines come into force.

Background

1. Trust in the reliability of the financial system is crucial for its proper functioning and a prerequisite if it is to contribute to the economy as a whole. Consequently, effective internal governance arrangements are fundamental if credit institutions and investment firms subject to Directive 2013/36/EU (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.

2. Over recent years there has been an increasing tendency by institutions and payment institutions to outsource activities in order to reduce costs and improve flexibility and efficiency. In the context of digitalisation and 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 prevalent outsourced activities. Notwithstanding its benefits, outsourcing of IT services and data poses security issues and challenges to institutions and payment institutions governance framework, in particular to internal controls as well as to data management and data protection.

3. Some institutions and payment institutions have increased the use of IT and fintech solutions and have launched respective projects to improve their cost efficiency as the intermediation margins from the traditional banking lending model are 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.

4. Outsourcing to cloud service providers gained rapidly importance in many industries. In 2017, the EBA addressed the specificities of outsourcing to the cloud by developing recommendations on outsourcing to cloud service providers[1], which were based on the 2006 CEBS outsourcing guidelines. The recommendations aimed to overcome the high level of uncertainty regarding supervisory expectations that applied to outsourcing to the cloud and that this uncertainty was forming a barrier to institutions using cloud services. The recommendations have been integrated in the present guidelines and will be repealed when the guidelines enter into force.

5. Outsourcing arrangements, in particular when the service provider is located outside the EU, create specific risks both for institutions and payment institutions and their competent authorities and must be subject to appropriate oversight. Any outsourcing that would result in the delegation by the management of its responsibility, altering the relationship and obligations of the institution and the payment institution towards their clients, undermining the conditions of their authorisation or removing or modifying any of the conditions subject to which the institution's and payment institution's authorisation was granted is not allowed. Outsourcing arrangements should not create undue operational risks or impair the quality and independence

[1]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.

of institutions and payment institutions internal controls or the ability of those and the competent authorities to supervise compliance with regulatory requirements.

6. [Empty Shell] The responsibility of the institutions' and payment institutions' management body can never be outsourced. Outsourcing must not lead to a situation where an institution or a payment institution becomes a so called "empty shell" that lacks the substance to remain authorised. To this end the management body should ensure that sufficient resources that appropriately support and ensure the performance of those responsibilities, including to oversee the risks and to manage the outsourcing arrangements, are available.

7. [Third Countries] Outsourcing is also relevant in the context of gaining or maintaining access to the EU financial market. Third countries institutions and payment institutions may wish to set up subsidiaries or branches in the EU in order to get or maintain access to EU 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 the EU, e.g. by relying on the outsourcing of processes, services or activities to the third country parent institution or other third country group entities.

8. [Third Countries] Competent authorities must grant authorisation in full compliance with Union law, should set a strict framework in line with these guidelines for the outsourcing from institutions and payment institutions in the EU to third country entities and ensure consistent and effective supervision. Competent authorities should also ensure that institutions and payment institutions have policies and procedures in place in order to comply with the relevant framework at all times.

Kommentar [MTU2]: Bitkom Comments: Outsourcing to „third countries" (Non-EU/EEA-states) and the rules tobe observed in that case should be addressed in further detail in the GL.

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

10. The guidelines should be read in conjunction with and 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 and the EBA guidelines on ICT risk assessment under the SREP.

11. 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 (PSD2), EBA guidelines on security measures for operational and security risks under PSD2 and EBA guidelines on major incident reporting under PSD2.

12. All requirements within the guidelines are subject to the principle of proportionality, meaning that they are to be applied in a manner that is appropriate, taking into account in particular the institution's and payment institution's size, internal organisation and the nature, scope and complexity of their activities.

Rationale and objective of the guidelines

13. The EBA is updating the CEBS guidelines on outsourcing issued in 2006, which only applied to credit institutions, in order to establish a more harmonised framework for the outsourcing arrangements of financial institutions. The scope of application covers not only credit institutions and investment firms subject to Directive 2013/36/EU (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[2] and to account information service providers that are only registered for the provision of service 8 of Annex I to PSD2. Outsourcing arrangements between institutions, payment institutions and such entities are within the scope of the guidelines, when they act as outsourcing service providers.

14. The update of the Guidelines takes into account and is consistent with the current requirements under Directives 2013/36/EU (CRD), 2014/65/EU (MiFID), 2009/110/EC (e-money Directive) and 2015/2366/EU (PSD2), 2014/59/EU (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 guidelines on step-in risk published by the Basel Committee on Banking Supervision (BCBS), have been taken into account.

15. Under Article 16 of Regulation (EU) No 1093/2010 (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 European Union law. In particular, requirements regarding outsourcing of banking activities by institution are not harmonised to the same extent as for institutions and payment institutions subject to MiFID II and PSD2.

16. Divergent regulatory approaches carry a risk of regulatory arbitrage, which may expose the European Union to financial stability risks. Those risks are particularly acute in relation to institutions and payment institutions outsourcing processes, services or activities (referred to as "functions") to third countries where supervisory authorities may lack the necessary powers and tools to adequately and effectively supervise service providers that provide such critical or important functions to EU institutions and payment institutions.

17. 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 supplementing MiFID II.

18. Article 109(2) of Directive 2013/36/EU requires parent undertakings and subsidiaries subject to this Directive to meet the governance requirements not only on a solo basis, but also on a consolidated or sub-consolidated basis, unless waivers have been granted under Article 21 of

[2] 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

Directive 2013/36/EU. It should be ensured that parent undertakings and subsidiaries subject to this Directive implement such arrangements, processes and mechanisms in their subsidiaries not subject to this Directive (e.g. payment institutions, e-money institutions, AIFMD and UCITS firms). Governance arrangements, processes and mechanisms must be consistent and well-integrated and those subsidiaries not subject to this Directive must also be able to produce any data and information relevant for the purpose of supervision.

Governance of outsourcing arrangements

19. Institutions and payment institutions should have sound internal governance arrangements, which include a clear organisational structure. Outsourcing arrangements are one aspect of institutions' and payment institutions' organisational structure. The guidelines include requirements that aim at ensuring that:

    a. there is effective day to day management by the management body[3];

    b. there is effective oversight by the management body;

    c. there are a sound outsourcing policy and 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;

    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 reintegration of the critical or important outsourced function; and

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

20. Institutions and payment institutions must determine whether the function to be outsourced is considered critical or important. The guidelines provide for criteria to ensure a more harmonised assessment of the criticality or importance of functions. 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 for the outsourcing of critical or important functions, aiming at ensuring the soundness of their governance arrangements and that competent authorities can exercise effective supervision.

21. Institutions and payment institutions use outsourcing based on business requirements and to achieve their strategic objectives. When outsourcing processes, services or activities to service

[3] Payment institutions should refer to definition of "management body" under the Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) published in December 2017in the EBA website: https://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-security-measures-under-psd2

providers, institutions and payment institutions must not only consider the ongoing costs, but also the need to oversee and control outsourced processes, services or activities and the risks that result from outsourcing.

22. While the guidelines focusses on outsourcing arrangements, 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. In order to manage all risks, institutions and payment institutions should assess the risks that result or may result from those arrangements, in particular their operational and reputational risk.

23. 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 risks posed by the outsourcing of critical or important functions to a limited number of service providers. The latter is in particular 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 concentration risks as well as the risk of creating empty shells that would lack the substance to remain authorised.

24. 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 competent authorities.

25. Institutions need to consider also the likelihood that they might be obliged to bail out service providers, if they depend heavily on their services. In this context, the Guidelines reflect the BCBS work on the step-in risk[4] that apply to large internationally active banks.

26. Each form of outsourcing has its specific risks and advantages. Intra-group 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 interests that may be caused by outsourcing arrangements, e.g. between different entities within the scope of consolidation.

27. Where institutions and payment institutions intend to outsource functions to entities within the same group, they should ensure that the selection of a group entity is based on objective reasons, 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 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

[4] The guidelines are available under the following link: https://www.bis.org/bcbs/publ/d398.htm

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.

28. Outsourcing to service providers located in third countries must be subject to additional safeguards that ensure that they do not lead to an undue increase of risks or impair the ability of competent authorities to effectively supervise institutions and payment institutions.

29. Outsourcing does not lower institutions and payment institutions obligation to comply with regulatory requirements and internal corporate values, e.g. 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 services providers are located in third countries.

30. 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 regards to critical or important ones, may impact institutions' and payment institutions' ability to manage their risks, such as operational risks, including compliance and reputational risks.

31. 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 encoded within the written outsourcing agreement.

32. Outsourcing arrangements also need to be considered in the context of institutions recovery and resolution planning, including their ability to continually have access to outsourced critical or important function while being in financial distress, restructuring or resolution. Business decision to outsource any functions should not in any way impede the resolvability of the institution.

33. The institutions', payment institutions' and competent 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 provide appropriate assurance that outsourced functions are provided as contractually agreed and in line with regulatory requirements. Further guidance is provided on how institutions and payment institutions can exercise to the audit rights in a risk-based manner, taking account of concerns regarding the organisational burden for both, the outsourcing institution and payment institution and the service provider, as well as of 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

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

(EU) 2016/679[5](GDPR). When outsourcing information technologies (IT) or data it is imperative that business continuity and data protection aspects 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, this includes also outsourced IT infrastructures and services.

35. 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. This triggers the need to require such arrangements also from some service providers and in particular regarding outsourced critical or important functions[6].

36. The EBA identified differences in national regulatory and supervisory frameworks for cloud outsourcing, for example with regard to the information requirements that institutions needed to comply with, and therefore issued in 2017 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 to cloud service providers and have been reflected accordingly in these guidelines. However, where appropriate and relevant, a few sections of these guidelines specify requirements applicable solely for cloud outsourcing.

37. 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 respective data and systems.

38. As cloud service providers often operate a geographically dispersed computing infrastructure that entails the regional and/or global distribution of data storage and processing, the guidelines set out specific requirements for data and data processing. Notwithstanding this guidance, 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.

[5] 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)

[6] The term critical or important is used in line with MiFID and PSD2 and replaces the term "material" that has been used in the previous guidelines.

39. 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.

40. The guidelines specify that sub-outsourcing requires ex ante notification to institutions and payment institutions in case of outsourcing of critical or important functions. When the outsourcing affects personal data, the consent of the institution and payment institution to sub-outsourcing is mandatory under the GDPR. 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

41. It is of particular importance that competent authorities have a comprehensive overview on outsourcing arrangements of institutions and payment institutions, to be able to exercise their supervisory powers. Institutions and payment institutions should therefore adequately inform competent authorities about planned outsourcing of critical or important function. In addition, institutions and payment institutions should also document all their outsourcings. To this end, the guidelines set out specific documentation requirements for institutions and payment institutions outsourcing arrangements.

42. Competent authorities need to identify concentrations of outsourcing arrangements at service providers. Concentration of outsourcing at important service providers or with regard to critical or important functions may in extreme cases lead to disruptions of the provision of financial services by multiple institutions. If important service providers, e.g. in the area of information technology or financial technology, fail or are not any longer able to provide their services, including in the cases of severe business disruptions caused by external events, this may cause even systemic risks to the financial markets.

43. The need to monitor and manage concentration risk is particularly relevant to certain forms of IT outsourcing, including cloud outsourcing, which are 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-REC/20XX/XX

DD Month YYYY

Draft Consultation Paper on 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[7]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions and payment institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/201x/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

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

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

2. Subject matter, scope and definitions

Subject matter

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

The wording "criticial or important functions" is based on the wording used under Directive 2014/65/EU (MiFID II) and the Commission delegated regulation (EU) 2017/565 supplementing MiFID II and is used only for the purpose of identifying services, activities or functions under outsourcing arrangement; this definition is without prejudice to the definition of "critical functions" under Article 2(1)(35) of 2014/59/EU (BRRD). In particular the delegated regulation (EU) 2017/565 specifies under its 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 (Solvency II), while Directive 2015/366 (PSD2) uses in the context of outsourcing "important function" for the purpose of identifying activities, services or functions under outsourcing arrangements for which specific requirements apply. Hence, to embrace all existing legislation and ensure a level playing field for credit institutions, investment firms, payment institutions and electronic money institutions, the wording used under MiFID II is therefore used within the guidelines.

6. The guidelines specify how the arrangements referred to in paragraph 5 of these guidelines should be reviewed and monitored by competent authorities in the context of Article 97 of Directive 2013/36/EU[8] (SREP assessment), Article 9 (3) of Directive (EU) 2015/2366[9], Article 5 (5) of Directive 2009/110/EC[10] 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, including the European Central Bank with regards to matters

[8] 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

[9] Directive (EU) 2015/2366 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

[10] 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

relating to the tasks conferred on it by Regulation (EU) No 1024/2013, 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 institution within the meaning of point 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".

Scope of application

9. Without prejudice to Directive 2014/65/EU (MiFID II), the Commissions delegated Regulation (EU) 2017/565 containing requirements regarding the outsourcing for institutions providing investment services and performing investment activities and respective guidance issued by the European Securities and Markets Authority regarding investment services and activities, institutions referred to in Directive 2013/36/EU should also comply with these guidelines on a solo basis, sub-consolidated basis and consolidated basis as set out in Articles 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. Competent authorities responsible for the supervision of institutions, payment institutions and electronic money institutions should comply with these guidelines.

Definitions

11. 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 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, or parts thereof that would otherwise be undertaken by the institution, the payment institutions or the electronic money institution itself.
Function	means any processes, services or activities, or parts thereof.

Critical or important function[11]	means any outsourcing of a function which is considered as critical or important including any operational tasks performed by the internal control functions.
Sub-outsourcing	means a situation where the service provider under an outsourcing arrangement further transfers a process, a service or an activity, or parts thereof, to another service provider.[12]
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.
Community cloud	means cloud infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group.
Hybrid cloud	means cloud infrastructure that is composed of two or more distinct cloud infrastructures.

Kommentar [MTU3]: Bitkom Comment: This definition should be deleted; it is mostly tautological. Rather, reference should be made to GL 9.1 and to Art 30 of the Delegated Regulation 2017/565 supplementing MiFID II.

3. Implementation

Date of application

12. These guidelines apply from 30 June 2019 [indicative date]. These guidelines apply to outsourcing arrangements entered into on or after [30 June 2019]. Institutions, payment institutions and electronic money institutions should use the next scheduled review or renewal date following the entry into force of these guidelines to revise and, if necessary, amend

Kommentar [MTU4]: Bitkom Comments: The guidelines should allow more time for industry players, i.e. institutions and service providers, to adapt to the new guidelines. 1 year „headroom" between the publication of the final guidelines and the application thereof would be reasonable.
EBA should keep in mind that institutions obliged to change existing outsourcing agreements find themselves in a difficult bargaining position, pressure from the regulator to conform with new guidelines and reluctance on the side of their service providers to adapt to the new guidelines.
1 year headroom for the implementation of compliant monitoring, preparation of the outsourcing register and GL-compliant risk management would be reasonable as well.

[11] The wording "criticial or important functions" is based on the wording used under Directive 2014/65/EU (MiFID II) and the 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 recovery and resolution framework as defined under Article 2(1)(35) of 2014/59/EU (BRRD).

[12] Sub-outsourcing has been referred to in other EBA documents also as chain of outsourcing or chain-outsourcing.

outsourcing agreements entered into before 30 June 2019 to ensure they are compliant with the Guidelines. The Guidelines will apply to these agreements from the point they are reviewed or renewed.

Transitional provisions

13. Institutions, payment institutions and electronic money institutions should complete the documentation of all existing outsourcing arrangements, other than outsourcing arrangements to cloud services providers[13], in line with these guidelines following the first renewal date of each existing outsourcing arrangement, but not later than by 31 December 2020.

Repeal

14. The CEBS Guidelines on Outsourcing of 14 December 2006 and the EBA Recommendation on outsourcing to cloud service providers[14] are repealed with effect from 30 June 2019 [indicative date].

Q1: Are the guidelines regarding the subject matter, scope, including the application of the guidelines to electronic money institutions and payment institutions, definitions and implementation appropriate and sufficiently clear?

4. Guidelines on Outsourcing

Title I – Proportionality and group application

1 Proportionality

15. Institutions, payment institutions and competent authorities should, when complying or monitoring compliance with these guidelines, have regard to the principle of proportionality. The proportionality principle aims at ensuring that institution's and payment institution's governance arrangements, including those related to outsourcing, are consistent with the nature, scale and complexity of their activities, so that the objectives of the regulatory requirements are effectively achieved.

16. When applying the principle of proportionality, institutions and competent authorities should take into account the criteria specified in Title I of the EBA Guidelines on Internal Governance

Kommentar [MTU5]: Bitkom Comments: „Proportionality" is an important issue as the burden of regulation otherwise becomes an obstacle for growth and development in the financial services market. This is important with respect to competitors from third countries as well as for a healthy internal market between smaller and larger players. Furthermore, EBA should keep in mind and should emphasize that proportionality has various dimensions (smaller vs. larger institutions, risky vs less risky activities). Here especially national CAs and other players (e.g. auditors) need more guidance. EBA should therefore further emphasize and explain in more detail the principle of proportionality. We ask EBA to specify proportionality criteria in various sections of these GL, in particular No. 24 (risk assessment), No 46 (register), No 41 (business continuity), No. 89 ss. (exit).

[13] Outsourcing to cloud service providers should be documented by 01 July 2018 in line with the recommendation on outsourcing to cloud service providers, that is available under the following link: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers.

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

in line with Article 74 (2) of Directive 2013/36/EU. Those criteria should be used mutatis mutandis also by payment institutions when applying the principle of proportionality[15].

2 Outsourcing within group application and institutional protection scheme

17. Institutions and payment institutions which are subsidiaries of an EU parent undertaking or of a parent undertaking in a Member State to whom no waivers have been granted on the basis of Articles 7 and 10 of Regulation (EU) No 575/2013 or of Article 21 of Directive 2013/36/EU should ensure that they comply with these Guidelines on an individual basis in accordance with Article 109 (1) of that Directive.

18. In accordance with Article 109(2) of Directive2013/36/EU, these Guidelines should apply on the sub-consolidated and consolidated basis. For this purpose, the EU parent undertakings and 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.

19. In accordance with paragraph 18:

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

    b. where the register of all existing outsourcing arrangements as referred to in Section 8, is established and maintained centrally within a group, the competent authorities, all institutions and payment institutions should be able to obtain their respective individual register without undue delay and it should be ensured by the institution or payment institution that all outsourcing arrangements, including outsourcing arrangements with service providers inside the group, are included in their individual register.

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

[15] Payment institutions should also refer to EBA Guidelines under PSD2 on the information to be provided for the authorisation of payment institutions and e-money institutions and the registration of account information service providers 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 .

20. In addition to points (a),(b),(c) of paragraph 19, institutions and payment institutions within a group, 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 arrangements within the same group or institutional protection scheme is being centralised (e.g. as part of a master agreement for the outsourcing arrangements), those institutions and payment institutions should ensure that there is independent monitoring of the service provider and an appropriate oversight by each institution or payment institution, including by receiving from the centralised monitoring function reports covering the institution's or payment institution's outsourcings. Those institutions and payment institutions should also ensure that their management body will be duly informed of relevant changes being planned regarding the centralised service providers in order for them to assess the impact of these changes and ensure compliance with all regulatory requirements;

    b. where those institutions and payment institutions within the group, institutions affiliated to a central body or part of an institutional protection scheme rely on a central pre-outsourcing assessment of the outsourcing arrangements as referred to in Section 9, each institution and payment institution should receive the respective assessment and ensure it takes into consideration its specific structure and risks within their decision making.

    c. where those institutions and payment institutions rely on an exit plan that has been established within the group, institutional protection scheme or the central body, all institutions and payment institutions should receive the respective plan, be satisfied that the plan can be effectively executed and consider it in their decision to make use of the outsourcing arrangement.

21. Where waivers have been granted on an individual basis on the basis of Articles 7 and 10 of Regulation (EU) No 575/2013 or of Article 21 of Directive 2013/36/EU, the provisions of these guidelines should be applied by the parent undertaking in a Member State for it and its subsidiaries or by the central body and its affiliates as a whole.

Q2: Are the guidelines regarding Title I appropriate and sufficiently clear?

Title II – Outsourcing arrangements

22. Institutions and payment institutions should establish whether an arrangement with a third party falls under the definition of outsourcing and, if so, whether or not it is an outsourcing of a critical or important function in accordance with Section 9.1 of the guidelines. When conducting the assessment w a, it is not relevant whether or not the institution or the payment institution has performed that function in the past or it would be able to perform it by itself.

Kommentar [MTU6]: Bitkom Comments: EBA should require that the institutions take ownership of the risk assessment and decisions of the central outsourcing department.

Kommentar [MTU7]: Bitkom Comments: It is unclear what is meant by "whether or not … it would be able to perform it by itself". It seems that the last half of the definition „… that would otherwise be undertaken by the institution … itself." should be interpreted such that (a) regulated functions that necessitate a license or other authorisation other than the institution's license should be carved out (e.g. central bank functions, central depositary functions, banking business for a payment institute), (b) services which do not form a direct part of or which are not rendered directly to enable services of the institution typical for the scope of license of the institution, should be carved out (e.g. services, goods, utilities listed in No 23).

23. The acquisition of services (e.g. advice of an architect regarding the premises, legal representation in front of the court and administrative bodies, servicing of company cars, catering), goods (e.g. purchase of office supplies, ~~or~~ furniture or general office software) or utilities (e.g. electricity, gas, water, telephone line, data communication network services, e-mail, fax and other general communciation facilities) that are not normally performed by the institutions or payment institutions are not considered outsourcing.

24. The risks, including in particular the operational risks, of all arrangements with third parties, including the ones referred to in paragraph 22 and 23, should be assessed in line with paragraphs 53 and 55 and Section 9.3, taking into account the application of the proportionality principle as referred in Section 1.

25. Without prejudice to the requirements within Title III, institutions and payment institutions should ensure that banking activities [16] or payment services that require authorisation or registration by a competent authority in the Member State where they are authorised are only outsourced to a service provider located in the same Member State or in another Member State, if one of the following conditions is met:

    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 services or activities in accordance with the relevant national legal framework.

26. Without prejudice to the requirements within Title III, institutions and payment institutions should ensure that banking activities or payment services that require authorisation or registration by a competent authority in the Member State where they are authorised are only outsourced to a service provider located in a third country if the following conditions are met:

    a. the service provider is authorised to provide that banking activity, or payment service in the third country and is effectively supervised by a relevant competent authority in that third country;

    b. there is an appropriate cooperation agreement in the form of a memorandum of understanding between the competent authorities responsible for the supervision of the institution and the supervisory authorities responsible for the supervision of the service provider;

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

        i. obtain on 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;

[16] See also Article 9 of Directive 2013/36/EU with regard to the prohibition against persons or undertakings other than

Kommentar [MTU8]: Bitkom Comments: As outlined in our previous comment, Bitkom favours to carve out services, goods and utlities that do not form a direct part of typical services of the institution. EBA should enhance the list of examples in order to capture a modern infrastructure of an institution

Kommentar [MTU9]: Bitkom Comments: BaFin draws a line between general software supply and support and suport for core banking software and or software products for central control functions. EBA should comment on this or confirm BaFin's position.

Kommentar [MTU10]: Bitkom Comment: It would be helpful for the market to receive further guidance on the application of the proportionality principle in this context.

Kommentar [MTU11]: Bitkom Comment: This guideline may be misunderstood in light of the current legal understanding of outsourcing. As of today, in an outsourcing structure the outsourcing service provider may undertake certain functions of regulated activities on behalf of the institution without the necessity for the service provider to obtain a license in this respect. This legal structure is highly important for FinTech companies many of whom use „white label banking", i.e. an outsourcing structure with a licensed institution, in order to deliver „their" services.

Kommentar [MTU12]: Bitkom Comment: Not only „national legal frameworks", but also European law allows performing regulated activities without a license: e.g. agents under PSD1/2 and e-money-agents under 2EMD.

credit institutions from carrying out the business of taking deposits or other repayable funds from the public.

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

iii. receive as soon as possible information from the supervisory authority in the third country for the purpose of 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;

iv. cooperate with the relevant supervisory authorities in the third country on enforcement in case of breach of 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 applicable regulatory requirements from the supervisory authorities in the third country as soon as practicable.

Q3: Are the guidelines in Title II and, in particular, the safeguards ensuring that competent authorities are able to effectively supervise activities and services of institutions and payment institutions that require authorisation or registration (i.e. the activities listed in Annex I of Directive 2013/36/EU and the payment services listed in Annex I of Directive (EU) 2366/2015) appropriate and sufficiently clear or should additional safeguards be introduced?

Title III – Governance framework

3 Governance requirements

27. Outsourcing of functions cannot result in the delegation of the management body's or bodies' responsibilities. Institutions and payment institutions remain fully responsible and accountable for complying with all of their regulatory obligations. In particular, the ability to oversee the outsourcing of critical or important function must always be retained by the institution and the payment institution.

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

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

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

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. the day to day management of the institution or payment institution, including the management of risks associated with the outsourcing; and

f. the oversight role of the management body in its supervisory function.

29. Outsourcing should not lower the suitability requirements applied to the members of an institution or payment's institution's management body, persons responsible for the management of the payment institution and its key functions holders. Institutions and payment institutions should retain adequate competence and sufficient skilled resources to ensure appropriate management and oversight of outsourcing arrangements.

30. Institutions and payment institutions should:

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

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

c. taking into account Section I of these Guidelines, should establish an outsourcing function or designate a senior staff member (e.g. Key Function Holders) who is directly accountable to the management body or at least ensure a clear division of task and responsibilities for the monitoring of outsourcing arrangement.

31. Institutions and payment institutions should maintain at all times a sufficient retained organisation and not be "empty shells" or "letter-box entities". To this end they should:

a. meet all the conditions of their authorisation [17] at all times, including for the management body to carry out effectively its responsibilities;

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

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

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

[17] 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; the implementing technical standards (ITS) under Article 8(3) of Directive 2013/36/EU on standard forms, templates and procedures for the provision of the information required for the authorisation of credit institutions.

For payment institutions, guidelines on the information to be provided for the authorisation of payment institutions under Directive 2015/2366/EU (PSD2).

Kommentar [MTU13]: Bitkom Comment: It is not clear what is meant by day to day management in this case. If EBA wishes to state that the management body of the institution is responsible for the day to day management of the institution in general this comment should be deleted since it is self-evident. If EBA wanted to state that the management is responsible for the day to day management of the outsourcing; the statement should be criticised as being an unreasonably high demand. The day to day management should be left to the outsourcing service provider.

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

    a. outsourcing arrangements do not impair the ability of the management body, including any specialised committees thereof, to carry out its duties;

    b. they can take and implement decisions related to their business activities and functions, including with regard to those which have been outsourced;

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

    d. internal control functions have sufficient authority, stature, resources and access to the management body to perform their tasks, including with regards to outsourcing arrangements;

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

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

    g. they retain with regard to the outsourcing of critical or important function at least one of the following abilities under going concern conditions, within an appropriate timeframe:

        i. transfer the critical or important function to alternative service providers; or

        ii. reintegrate the critical important or important function;

    h. where sensitive data, including personal data, is processed or transferred to service providers located in both the European Union and/or third countries, appropriate measures are implemented and data is stored and processed in accordance with Regulation 2016/679.

4 Outsourcing Policy

33. The management body of institutions and payment institutions[18] should approve and maintain a written outsourcing policy and ensure its implementation, where applicable, on a consolidated, sub-consolidated and individual basis. For institutions, the outsourcing policy should be in accordance with Section 4 of the EBA's Guidelines on Internal Governance and

[18] See also EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (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

Kommentar [MTU14]: Bitkom Comment: EBA should consider outsourcing structures where institutions purchase standardised services or products in muti-client environments and will therefore - for efficiency and cost reasons - not be able to retain the possibility to implement specific solutions for their business activities.

Kommentar [MTU15]: Bitkom Comment: The term „FinTech" is not helpful in this context, as it does not add anything further to the term ICT, i.e. FinTech is included in the term ICT. We suggest to delete these words.

Kommentar [MTU16]: Bitkom Comment: Here and in further places GL require the institution to plan for the exit of the outsourcing service provider. EBA should define here or elsewhere what „appropriate timeframe" means. From Bitkom's point of view, the question of the transfer timeframe is secondary to the questions whether and how the outsourced functions can be maintained in a crisis of the service provider. This can be done by various means, including monitoring of the service provider and its critical personal and systems, planning for an insolvency of the service provider including bail out.

Kommentar [MTU17]: Bitkom Comment: EBA should make clear that conceiving an outsourcing policy highly depends on the size and on the structure of the institution, i.e. proportionality should apply. A smaller institution or an institution conducting only smaller business or very specialized business may have to react quite flexibly to the outsourcing offerings of service providers and may have to purchase mostly standardised services or products. An outsourcing policy should not unreasonably bind management and staff of an institution to procure services in a flexible manner.

take into account the requirements set out in Section 18 (new products and significant changes) of these EBA Guidelines[19].

34. The policy should consider 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, business lines, internal control functions and other individuals in respect of outsourcing arrangements in line with paragraph 30;

    b. the planning of outsourcing arrangements, including:

        i. the definition of business requirements regarding outsourcing arrangements;

        ii. the criteria, including those referred to in Section 9.1 and processes for identifying critical or important functions;

        iii. due diligence checks on prospective service providers, including the measures required under Section 9.2;

        iv. risk identification, assessment and management in accordance with Section 9.3;

        v. procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with Section 5;

        vi. business continuity planning in accordance with Section 6;

        vii. involvement of the management body, including, as appropriate, in the decision making on outsourcing; and

        viii. approval process of new outsourcing arrangements;

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

        i. the ongoing assessment of the service provider's performance in line with Section 11;

        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 renewal processes;

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

d. the documentation and record-keeping, which should take into account the requirements in Section 8;

e. the exit strategies and termination processes, including:

i. procedures to deal with service interruptions or unexpected termination of an agreement; and

ii. a requirement for a documented exit plan for each critical or important function to be outsourced.

35. The outsourcing policy should differentiate between the following:

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

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

c. intra group 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 the EU/EEA and outside the EU/EEA.

36. Institutions and payment institutions should ensure that the policy covers the potential effects of critical or important outsourcing arrangements on the risk profile, the ability to oversee the service provider and to manage the risks, the business continuity measures and on the institution's and payment institution's performance are identified and taken into account in the decision making process.

Q4: Are the guidelines in Section 4 regarding the outsourcing policy appropriate and sufficiently clear?

5 Conflicts of interest

37. Institutions, in line with Title IV Section 11 of the EBA guidelines on internal governance[20], and payment institutions should identify, assess and manage conflicts of interests with regard to their outsourcing arrangements.

38. Where outsourcing creates material conflicts of interest, including between entities within the same group, institutions and payment institutions need to take appropriate measures to manage those conflicts of interest. With regard to identified conflicts of interests, institutions and payment institutions should ensure that the decision on the outsourcing arrangement and

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

the oversight on the outsourcing arrangement are performed with a sufficient level of objectivity in order to appropriately manage conflicting interests. To this end, institutions should ensure that the conditions, including financial conditions, for the outsourced service are set at arm's length.

6 Business continuity plans

39. 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[21], and payment institutions should have in place appropriate business continuity plans with regard to the outsourcing of critical or important function.

40. Where the failure by the service provider to provide the critical or important function would lead to a severe business disruption, institutions and payment institutions should involve the service provider in its business continuity planning and establish, implement and maintain business contingency plans for disaster recovery. Such plans should be tested periodically, including the testing of backup facilities, and involve the service provider, when it is part of such plans.

Kommentar [MTU18]: Bitkom Comment: EBA should add „where applicable". Not all service providers will use backup facilities. In many cases data storage is run on active / active servers. EBA should rather make sure that the overall criteria is assuring availability.

41. Institutions and payment institutions should plan and implement arrangements to maintain the continuity of their business in the event that the quality of the outsourcing of the critical or important function deteriorates to an unacceptable level or that there is a material risk that the service level will fail or that the quality of the critical or important function will deteriorate to an unacceptable degree. 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.

Kommentar [MTU19]: Bitkom Comment: See comment on No 32g.

7 Internal audit function

42. The internal audit function's activities should cover, following a risk based approach, the independent review of outsourced activities. The audit plan[22] and programme should include in particular the outsourcing arrangements of critical or important function, including the appropriateness of data protection measures, controls, risk management and business continuity measures implemented by the service provider.

43. As referred to in Section 10.3 of these guidelines, institutions and payment institutions should ensure that information and audit rights are sufficiently ensured in particular for the outsourcing of critical or important functions and that the internal audit function is able to effectively enforce such audit rights.

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

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

[22] The audit plan should be approved by the audit committee, when such a committee has been established.

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

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

c. the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain within the risk appetite;

d. the risk appetite, risk management and control procedure of the service provider are in line with the institution's or payment institutions' strategy;

e. the appropriate involvement of governance bodies; and

f. the appropriate monitoring and management of outsourcing arrangements.

45. All audit recommendations and findings regarding outsourcing arrangements should be subject to a formal follow-up procedure. The institution and the payment institutions should ensure and document their effective and timely resolution.

Q5: Are the guidelines in Sections 5-7 of Title III appropriate and sufficiently clear?

8 Documentation requirements

46. Institutions and payment institutions should maintain a register of all outsourcing arrangements at institution and group level where applicable as referred to in Section 2, document and record all current outsourcing arrangements, distinguishing the outsourcing of critical or important functions and other outsourcing arrangements. Taking into account Title I of these Guidelines, for institutions and payment institutions within a group, institutions permanently affiliated to a central body, or institutions which are members of the same institutional protection scheme, the register may be kept centrally, provided that the section of the register relating to each individual institution can be obtained in a timely manner.

47. The documentation should include at least the following information for all existing outsourcing arrangements[23]:

a. with regard to the outsourcing arrangement:

i. a reference number for each outsourcing arrangement;

[23] Institutions and payments institution may take into account the template in Annex X

Kommentar [MTU20]: Bitkom Comment: EBA should require the full scale outsourcing register (compliant with all requirements of GL 8 only for outsourcing of critical or important functions. For other outsourcing arrangements a lesser (risk based reduction of) documentation should be sufficient. This would also be a demand of proportionality.

Kommentar [MTU21]: Bitkom Comment: Term should be identical to the one used in Art 113(7) CRR.

Kommentar [MTU22]: Bitkom Comment: EBA should make clear that the outsourcing register is an internal register first of all. Bitkom would like to stress that the information contained in the register may in many cases be considered as business secret of the institution and therefore access to the register must be limited.

Kommentar [MTU23]: Bitkom Comment: EBA should require the institutions to maintain the register in a generally available digital format.

ii. a brief description of the function that is outsourced;

iii. whether it is considered critical or important, the reasons why it is considered as such and the date of the last respective assessment;

iv. whether or not personal and confidential data is processed, transferred or held by the service provider[24];

v. the institutions and other entities within the scope of prudential consolidation that make use of the outsourcing agreement, including their names;

b. with regard to the service provider and, where applicable, all sub-service providers:

i. their name and registered address;

ii. the country of registration and LEI, or if unavailable, corporate registration number;

iii. their parent company, where applicable;

iv. whether or not the service provider or sub-service provider is part of the institution's group, based on the accounting scope of consolidation;

v. the country or countries in which the outsourced function will be performed by the service provider or the sub-service provider;

vi. the country or countries where data will or will potentially be stored;

c. in addition, the register should include at least the following information with regard to the outsourcing of critical or important functions and outsourcing to cloud service providers:

i. the date of the last risk assessment and a brief summary of the main results;

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

iii. the governing law of the outsourcing agreement;

iv. the commencement date and, as applicable, the expiry date and/or notice periods;

v. the date of the last and next scheduled audit, where applicable;

Kommentar [MTU24]: Bitkom Comment: EBA should allow to simply refer to the documentation on the pre-outsourcing due diligence and risk assessment.

Kommentar [MTU25]: Bitkom Comment: The name of a parent company may not be helpful in many cases where the service provider is part of a group structure. EBA should allow to simply refer to the documentation on the pre-outsourcing due diligence, if it includes an assessment of the service provider's group structure.

Kommentar [MTU26]: Bitkom Comment: EBA should allow to simply reference the documentation on the pre-outsourcing due diligence and risk assessment.

[24] Regulation (EU) 2016/679

vi. an assessment of the service provider's substitutability and/or the possibility to reintegrate the critical or important function back into the institution or the payment institution;

vii. identification of alternative service providers in line with point (vi);

viii. whether the outsourcing of the critical or important function is considered time critical;

ix. 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 locations where such data will be stored; and

x. the estimated yearly budget cost.

Kommentar [MTU27]: Bitkom Comment: It is not clear what „time critical" means in this context.

Q6: Are the guidelines in Sections 8 regarding the documentation requirements appropriate and sufficiently clear?

Title IV – Outsourcing process

9 Pre – outsourcing analysis

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

a. assess whether the planned outsourcing concerns a critical or important function in accordance with Section 9.1;

b. undertake appropriate due diligence on the prospective service provider in accordance with Section 9.2;

c. identify and assess all relevant risks of the outsourcing arrangement in accordance with Section 9.3;

d. identify and assess conflicts of interest that the outsourcing may cause in line with Section 5;

e. consider the consequences of where the service provider is located (within or outside the EU);

f. consider whether the service provider is part of the institution's accounting consolidation group and, if so, the extent to which the institution controls it or has the ability to influence its actions in line with Section 2.

9.1 Assessment of the criticality or importance

49. Institutions and payment institutions should always consider a function as critical or important for the purpose of outsourcing:

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

        i. their continuing compliance with the conditions of their authorisation under Directive 2013/36/EU , Regulation (EU) No 575/2013, 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 payments services and activities;

    b. when operational tasks of internal control functions are outsourced; or

    c. when they intend to outsource banking or payment services requiring authorisation by a competent authority as referred in Title II.

50. In the case of institutions, particular attention should be given to the assessment of the criticality or importance, when outsourcing activities, processes or services related to core business lines and critical functions as defined in Article 2(1)(35) and 2(1)(36) of Directive 2014/59/EU and identified by institutions using the criteria in Articles 7 and 8 of Commission Delegated Regulation (EU) 2016/778. Outsourcing arrangements regarding activities, processes or services relating to core business lines and critical functions should always be considered as critical or important for the purpose of these guidelines.

51. When assessing whether or not an outsourcing arrangement is critical or important, i.e. it concerns a critical or important function, institutions and payment institutions should take into account at least the following criteria:

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

    b. the potential impact of any disruption or outage of the outsourcing arrangement 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), legal and reputational risks;

iv. where applicable, recovery and resolution planning, resolvability and operational continuity in a resolution situation.

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

i. identify, monitor and manage all risks;

ii. comply with all legal and regulatory requirements; and

iii. conduct audits regarding the outsourcing arrangement;

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

e. taking into account other outsourcing arrangements, in accordance with Section 9.3, the institution's and payment institution's aggregated exposure to the same service provider or the cumulative impact of outsourcing arrangements in the same business area;

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

g. the possibility of the proposed outsourcing arrangement to be scaled up at the discretion of either party 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 difficulties, costs and timeframe for doing so ('substitutability');

i. the ability to reintegrate the outsourced function into the institution or the 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 the payment institution and their clients, including but not limited to Regulation 2016/679.

52. Where the institution or payment institution concludes that the outsourcing arrangement is not substitutable in an appropriate time frame or that its substitution would lead to a material business disruption, it should assess the overall impact of the disruption of the service on its financial position and on the orderliness of its business conduct.

Q7: Are the guidelines in Sections 9.1 regarding the assessment of criticality or importance of functions appropriate and sufficiently clear?

9.2 Due diligence

53. Before entering into an outsourcing arrangement, institutions and payment institutions should ensure in their selection process and assessment that the service provider has appropriate and sufficient ability, capacity, resources, organisational structure and, if applicable, required

Kommentar [MTU28]: Bitkom Comments: Under the assumption that the institution would otherwise provide the (same) services itself (see definition), the outsourcing should not have any impact on the services towards clients. EBA should therefore clarify that an analysis of the impact of unavailability or poor quality of the outsourced service must be taken into account. Also, EBA should add „if any", as there may not be any impact oft he services at all, e.g. if back office functions are outsourced.

Kommentar [MTU29]: Bitkom Comments: It is unclear what „size and complexity" relates to. Is this related to an institution's size? Does EBA envisage a critcial absolute size of a business area, such that proportionality plays a role in this assessment, e.g. in smaller institutions also relatively (relative to the size of the institution) large areas can be outsourced without being critical?

Kommentar [MTU30]: Bitkom Comment: See above comment on No 32g.

Kommentar [MTU31]: Bitkom Comment: EBA should add „infrastructure, in particular software, systems etc."

regulatory authorisation(s) to perform the critical or important function in a reliable and professional manner over the duration of the proposed contract.

54. Additional factors to be considered, when conducting due diligence on a potential service provider, include, but are not limited to its business model, nature, scale, complexity, financial situation, and, if applicable, group structure.

55. Where outsourcing involves the transfer, processing and storing of personal or confidential data, institutions and payment institutions should be satisfied that the service provider implements appropriate technical and organisational measures. In the case of personal data, data transfer, processing and storing should be done in compliance with the Regulation (EU) 2016/679. [25]

56. 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 a socially responsible manner and adheres to international standards on human rights, environmental protection and appropriate working conditions, including the prohibition of child labour.

Q8: Are the guidelines in Section 9.2 regarding the due diligence process appropriate and sufficiently clear?

9.3 Risk assessment of outsourcing arrangements

57. Institutions and payment institutions, taking into account the principle of proportionality in line with Section 1, should identify, manage, monitor and report all risks they are or might be exposed to relating to arrangements with third parties, regardless of whether or not those arrangement are considered outsourcing arrangement.

58. Institutions and payment institutions should assess the potential impact of the outsourcing arrangements on their operational risk based also on scenarios of possible risk events and should take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements. The assessment should include, where appropriate, high severity operational risk events. Within the scenario analysis institutions and payment institutions should assess the potential impact of failed or inadequate services received, including the risks caused by processes, systems, people or external events. Institutions and payment institutions, taking into account the principle of proportionality as referred in Section I, should document the scenario analysis performed and their result and estimate the extent to which the outsourcing arrangement would increase or decrease their operational risk.

[25] 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)

59. When assessing the risks of an outsourcing arrangement, institutions and payments institutions should balance the expected advantages of the proposed outsourcing arrangement, including any risks which can be managed and mitigated against any potential risks which 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, non-easily substitutable service provider; and

        ii. multiple outsourcings to the same or related service providers;

    b. the aggregate risks from outsourcing a large number of functions across the institution or payment institution and, in the case of institutions, the aggregate risks on a consolidated basis;

    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 and payment institution and at the service provider to manage and mitigate the risks.

60. 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 than 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 the competent authority to effectively supervise them.

61. In carrying out the risk assessment prior to the outsourcing and during ongoing monitoring of the service provider's performance institutions and payment institutions should, at a minimum:

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

    b. conduct a thorough risk-based analysis of the functions and related data and systems which are under consideration to be outsourced or have been outsourced;

    c. address the potential risk impacts, including legal and compliance risks, and 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;

Kommentar [MTU32]: Bitkom Comment: Please note that „dominant" and „not easily substitutable" are two different topics.

Kommentar [MTU33]: Bitkom Comment: We suggest to add performance risks and disruption risks as separate categories of material risks.

Kommentar [MTU34]: Bitkom Comment: We suggest to replace „sensitivity" by „criticality".

d. include considerations on the wider 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 the respect of the urgent recovery of the institution's and payment institution's data in particular; and

e. define and decide on an appropriate level of protection of data confidentiality, continuity of activities outsourced and 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.

Q9: Are the guidelines in Section 9.3 regarding the risk assessment appropriate and sufficiently clear?

10 Contractual phase

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

63. The outsourcing agreement should set out at least for all outsourcing arrangements:

   a. a clear description of the outsourced function;

   b. the start and end dates of the agreement, including notice periods;

   c. the governing law of the outsourcing arrangement;

   d. whether the sub-outsourcing of a critical or important function is permitted and if so, the agreement should ensure that the sub-outsourcing is subject to conditions specified in Section 10.1;

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

   f. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as further specified in Section 10.2;

Kommentar [MTU35]: Bitkom Comment: We suggest to rephrase this such that the assessment concerns the „impact on the services", i.e. the impact that the aplplicable local law, the enforcement provisions and insolvency laws might have on the provision of the services by the outsourcing service provider.

Kommentar [MTU36]: Bitkom Comment: We suggest to shorten or delete this GL. It is in large parts not necessary from a regulatory point of view to prescribe how institutions should structure their contractual relationship. EBA should shorten this in ordert o only address items which are really relevant from a supervisory perspective, such as audit rights.

Kommentar [MTU37]: Bitkom Comment: In case, contrary to the recommendation above to delete or to considerably shorten GL 10, EBA wishes to uphold this GL 10 No 63e: In many cases technical service providers may for security reasons not disclose the location of their data centres. In those cases even audits will be conducted in a manner that the auditor will not get to know the exact location of the data centre. EBA should amend the text here as follwos: „location, as far as it can be disclosed in accordance with applicable policies".

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

h. the unrestricted right of institutions, payment institutions and competent authorities to get any information needed with regard to the outsourcing and to access and audit the service provider as further specified in Section 10.3;

64. In addition, for the outsourcing of critical or important function, the following should be covered:

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

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

c. 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 carry out effectively the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirement;

d. the respective parties' financial obligations;

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

f. requirements to implement and test business contingency plans;

g. termination rights as further specified in Section 10.4;

h. provisions that ensure the access to data that are owned by the institution or the payment institutions in case of the insolvency of the service provider;

i. a clear statement that in the event of insolvency or discontinuing of business operations by either party the relevant data will be made available irrespective of the occurrence of the default; and

j. 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.

Kommentar [MTU38]: Bitkom Comment: In case, contrary to the recommendation above to delete or to considerably shorten GL 10, EBA wishes to uphold this GL 10 No 64: EBA could add: „(including the financial stability and any changes in management of the service provider)".

10.1 Sub-outsourcing of critical or important functions

65. The outsourcing agreement should specify whether or not sub-outsourcing of critical or important function is permitted. If so, it 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 in order to ensure that all contractual obligations between the service provider and the institution or the payment institution are still met;

    d. require the service provide to obtain prior approval from the institution and the payment institution before sub-outsourcing data subject to the GDPR;

    e. include an obligation for the service provider to inform the institution or the payment institution of any planned sub-outsourcing, or material changes thereto, 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 to the sub-contractors and the respective notification period;

    f. the notification period to be set under point (e) should allow the outsourcing institution and payment institution to carry out a risk assessment of the proposed changes before the changes come into effect;

    g. ensure, where appropriate, that the institution or the payment institution has the right to object against intended sub-outsourcing or that an explicit approval is required;

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

66. Institutions and payment institutions should only agree to sub-outsourcing, 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.

67. 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

Kommentar [MTU39]: Bitkom Comment: Should the EBA, contrary to the recommendation above to delete or to considerably shorten GL 10, uphold this GL 10 No 65: The intention of EBA seems to be to address the sub-outsourcing agreement here. In that case the word „terminate“ should be replaced by „require to terminate“.

institution. If a proposed sub-outsourcing could have material adverse effects on the critical or important outsourcing arrangement or lead to a material increase of risk, including where the conditions in paragraph 66 are not met, the institution and the payment institution should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.

10.2 Security of data and system

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

69. 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.

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

71. Without prejudice to the requirements under the GDPR, institutions and payment institutions, when outsourcing, including 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).

10.3 Access, information and audit rights

72. Institutions and payment institutions should ensure, within the written outsourcing agreement, that the service provider grants them and their competent authorities and any other person, including the statutary auditor, appointed by the institution, the payment institution or the competent authorities the following:

    a. complete access to all relevant business premises (head offices and operations centres), including the full range of devices, systems, networks, information and data used for providing the outsourced process, service or activity, financial information, personnel and the service provider's external auditors ('access 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 comply with all applicable regulatory requirements.

Kommentar [MTU40]: Bitkom Comment: EBA should clarify for multi-client servicer providers (the majority of all cases) that access is to be granted „as far as necessary for the inspection".

Kommentar [MTU41]: Same as before.

73. Institutions and payment institutions should ensure that the outsourcing agreement or any other contractual arrangements do not impede or limit the effective exercise of access and audit rights by them, competent authorities or third parties appointed by either to exercise these functions. Institutions and payment institutions should exercise their access and audit rights on a risk-based approach and adhere to applicable national and international standards.[26]

74. Without prejudice to their final responsibility, institutions and payment institutions may use third-party certifications and third-party reports made available by the service provider for the audits. However they should not rely solely on those.

75. Institutions and payment institutions may also use 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, in order to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider. Institutions and payment institutions should only make use of these methods where they:

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

    b. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the report is not obsolete and 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;

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

    d. 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);

    e. have the contractual right to request the expansion of the scope of the audits, 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

    f. retain the contractual right to perform individual audits at their discretion.

76. In line with the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process institutions should, where relevant, ensure the ability to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security

[26] See also Section 22 of the EBA guidelines on internal governance.

Kommentar [MTU42]: Bitkom Comments: Especially in multi client environments, it has become increasingly difficult for service providers to admit single audits; therefore third-party audit (by independent auditors, also in the form of pooled audits (see below)) have become a commonly used and efficient tool. EBA should clarify that institutions may rely on third party certifications plus the underlying audit reports within the scope of the certification, if it is up to date.

Kommentar [MTU43]: Bitkom Comment: Bitkom strongly favours that institutions should have the possibility to pool audit activities in certain fields of standardised services and products rendered to those institutions. Bitkom favours the standardisation of pooled audits by these EBA guidelines. Pooled audits are and should be a cost and time efficient tool to fulfil regulatory audit requirements.

Kommentar [MTU44]: Bitkom Comment: Bitkom asks EBA to add the „the right to request the expansion of the audits“ here.

measures and processes.[27] Taking into account Title I, payment institutions should also have internal ICT control mechanisms, including ICT security control and mitigation measures.

77. Institutions, payment institutions and competent authorities, auditors or third parties acting for the institution, payment institution or competent authorities should, before a planned onsite visit, provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would otherwise jeopardise the objective of the audit.

78. Institutions and payment institutions should make sure that service providers cooperate fully with competent authorities, their auditors or relevant third parties, in particular, in the context of onsite visits.

79. If the performance of audits or the use of certain audit techniques, such as pooled audits, may create a risk for another client's environment (e.g. in public clouds), alternative ways to provide a similar level of assurance required by the institution or the payment institution should be agreed on.

Kommentar [MTU45]: Bitkom Comment: EBA should provide best practice examples for the sufficient avoidance of such risks. As an example; pooled audits will usually be conducted by third parties professional service providers such as CPAs or specialised IT consultants. In order to avoid confidentiality risks for another client's environment, EBA should clarify that professional or contractual secrecy obligations undertaken by the auditor vis-a-vis the institutions and the outsourcing service provider should suffice.

80. 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 – either its internal auditors, the pool of auditors or external auditors acting on its behalf – have appropriate relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies, where applicable, to any staff of the institution or payment institution reviewing third-party certifications or audits carried out by service providers.

10.4 Termination rights

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

    a. the provider of outsourced services is in a material breach of applicable law, regulation, or contractual provisions;

    b. identified impediments capable to substantially alter the performance of the outsourced service;

    c. there are material changes affecting the outsourcing arrangement or the service provider (such as sub-outsourcings or changes of sub-contractors);

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

Kommentar [MTU46]: We suggest to delete this GL 10.4. EBA might instead require the institutions to foresee „appropriate" termination rights. Should the EBA, contrary to the recommendation above to delete or to considerably shorten GL 10.4, wish to uphold this GL 10.4 No 81: EBA should make clear that not „any" breach etc. must lead to a termination right for of the outsourcing agreement. That does not seem to be reasonable. Also, institutions will in many cases face strong opposition of service providers when trying to implement such extensive termination rights in an outsourcing agreement.

[27] 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

e. instructions of the institution or payment institution's competent authority, e.g. in the case that the competent authority is not in the position to effectively supervise the the institution or the payment institution.

82. The outsourcing arrangement should facilitate the transfer of outsourced function to another service provider or the reincorporation into the institution or the payment institution. To this end the written outsourcing arrangement should:

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

b. 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 to the institution or payment institution, including the treatment of data; and

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

Q10: Are the guidelines in Section 10 regarding the contractual phase appropriate and sufficiently clear; do the proposals relating to the exercise of access and audit rights give rise to any potential significant legal or practical challenges for institutions and payment institutions?

11 Oversight of outsourced functions

83. Institutions and payment institutions should monitor on an ongoing basis the performance by the service provider and, where applicable sub-contractors, with regard to all outsourcing arrangements with a particular focus on the outsourcing of critical or important functions, including that the availability, integrity and security of data and information is ensured.

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

85. Institutions should regularly update their risk assessment in accordance with Section 9.3 and periodically report to the management body on any risks identified in respect of outsourcing of critical or important function.

86. Institutions and payment institutions should monitor and manage their own concentration risk caused by outsourcing arrangements, taken into account Section 9.3 of these guidelines.

87. Institutions and payment institutions should ensure that outsourcing arrangements meet appropriate performance and quality standards in line with their policies on an ongoing basis by:

a. ensuring they receive appropriate reports from service providers;

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

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

88. 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, if necessary with immediate effect.

Q11: Are the guidelines in Section 11 regarding the oversight on outsourcing arrangements appropriate and sufficiently clear?

12 Exit strategies

89. Institutions and payment institutions should have a clearly defined exit strategy for all outsourcing of critical or important functions in line with their outsourcing policy, taking into account at least the possibility of the termination of outsourcing arrangements, the failure of the service provider and a material deterioration of the service provided.

90. Institutions and payment institutions should ensure that they are able to exit outsourcing arrangements, without undue disruption of their business activities or adverse effects on their compliance with the regulatory framework and without 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 sufficiently tested (e.g. by carrying out an analysis of the potential costs, impact, resource and timing implications of transferring an outsourced service to alternative provider); and

b. identify alternative solutions and develop transition plans to enable the institution or payment institution to remove and transfer outsourced functions and data from the service provider to alternative providers or back to the institution or the payment institution in a controlled and sufficiently tested manner, taking into account data location issues and maintenance of business continuity during the transition phase.

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

a. define the objectives of the exit strategy;

b. perform a business impact analysis commensurate with the risk of the outsourced processes, services or activities, to identify 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 indicators to be used for the monitoring of the outsourcing arrangement under Section 11, including such based on unacceptable service levels, that can trigger the exit.

Q12: Are the guidelines in sections 12 regarding exit strategies appropriate and sufficiently clear?

13 Duty to adequately inform supervisors

92. Institutions and payment institutions should make available the register of all existing outsourcing arrangements to the competent authority in a common data base format within each supervisory review and evaluation process, but at least every 3 years and in any case on request by the competent authority.

93. Institutions and payment institutions should adequately inform competent authorities in a timely manner of planned outsourcing of critical or important functions, including the outsourcing of critical or important cloud services, before they intend to enter into the new outsourcing agreement and make available to competent authorities at least the information under points (a), (b) and, where available, (c) of paragraph 47.

94. Institutions and payment institutions should adequately and promptly inform competent authorities where a function under an existing outsourcing arrangement became critical or important. The communication to competent authorities should include the information in paragraph 93 and:

    a. the reference number within the register;

    b. the last contract renewal date (where available); and

    c. the service expiry date or next contract renewal date (where available).

95. Institutions and payment institutions [28] should inform without undue delay competent authorities of material changes and severe events regarding their outsourcing arrangements

Kommentar [MTU47]: Bitkom-Comment: EBA should not install via these guidelines any new notification requirement currently not foreseen under applicable regulation, e.g. for credit institutions in Germany.

[28] See also EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2), available under: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

which could have a material impact on the continuing provision of the institutions and payment institutions' business activities,

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

Q13: Are the guidelines in Section 13 appropriate and sufficiently clear, in particular, are there any ways of limiting the information in the register which institutions and payment institutions are required to provide to competent authorities to make it more proportionate and relevant? With a view to bring sufficient proportionality, the EBA will consider the supervisory relevance and value of a register covering all outsourcing arrangements within each SREP cycle or at least every 3 years in regard of the operational and administrative burden.

Title V – Guidelines on outsourcing addressed to competent authorities

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

Kommentar [MTU48]: Bitkom Comment: It seems that EBA should not refer to the historic scope of a license in this place, but rather to the existing / current license.

98. Competent authorities should be satisfied that they can effectively supervise institutions and payment institutions, including that institutions or payment institutions have ensured within the outsourcing arrangement that service providers are obliged to grant the competent authority and the institution audit and access rights in line with Section 10.3.

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

100. Further to the information provided within the register as referred to in Section 8 and information provided in line with Section 13, competent authorities may ask institutions and payment institutions for additional information on their risk analysis, in particular for critical or important outsourcing arrangements, such as:

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

b. whether the outsourcing institution or payment institution has an exit strategy in case of termination by either party or disruption of the provision of the services; and

c. whether the outsourcing institution or payment institution maintains the skills and resources necessary to adequately monitor the outsourced activities.

101. Competent authorities should assess on a risk based approach:

a. whether institutions and payment institutions monitor and manage appropriately any outsourcing arrangement and in particular those that are critical or important;

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

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

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

102. Competent authorities should ensure that EU/EEA institutions and payment institutions are not operating as an 'empty shell', including where institutions use back-to-back transactions or intragroup transactions to transfer a part of the market risk and credit risk to a non-EU/EEA entity and that they have appropriate governance and risk management arrangements in place to be able to take on identification and management of the risks that they have generated, and that in the event of a crisis, they could rapidly deploy scaled up risk management arrangements.

103. Within their assessment competent authorities should take into account all risks and in particular[29]:

a. the operational risk[30] posed by the outsourcing arrangement;

b. reputational risk;

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

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

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

f. the extent to which the outsourcing institution or payment institutions controls the service provider or has the ability to influence its actions, the reduction of risk that may

[29] For CRD institutions, see also EBA guidelines on SREP

[30] See also EBA guidelines on ICT risk

result from a higher level of control and the extent to which the service provider is included in the consolidated supervision of the group; and

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

104. Where concentration risks are identified, competent authorities should monitor the development of such risks and evaluate their potential impact on other institutions and payment institutions and the stability of the financial market.

105. Where concerns are identified that lead to the assessment that institutions and payment institutions do not any longer have robust governance arrangements in place or do not comply with regulatory requirements, competent authorities should take appropriate action, which may include limiting or restricting the scope of the functions outsourced or requiring exit from one or more outsourcing arrangements. In particular, taking into account the need of the institution and payment institutions to operate on a continuous basis, cancellation of contracts could be required, if the supervision and enforcement of regulatory requirements cannot be ensured by other measures.

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

Q14: Are the guidelines for competent authorities in Title V appropriate and sufficiently clear?

Annex 1 – Documentation of outsourcing

With regard to the expected minimum content of the register in which all outsourcing should be documented please refer to Section 8 and to the illustrative template provided in a separate Excel file.

Q15: Is the template in Annex I appropriate and sufficiently clear?

5. Accompanying documents

5.1 Draft cost-benefit analysis / impact assessment

Article 16(2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) (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, only applied to credit institutions and needed to be replaced by EBA guidelines in order to establish a more harmonised framework for the outsourcing arrangements of all financial institutions in the scope of its action. The update is necessary to take into account changes within EU legislation, but also to broaden the scope of application of the Guidelines to not only credit institutions and investment firms subject to Directive 2013/36/EU but also to payment institutions subject to Directive 2015/2366/EU and electronic money institutions subject to Directive 2009/110/EC. Outsourcing to third countries may change in volume after the UK has notified their intention to leave the European Union. In addition, scope and nature of outsourcing arrangements have changed over time and in particular outsourcing of IT processes and infrastructures became more common. 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, in particular if no additional safeguards are implemented.

B. Policy objectives

To ensure a level playing field and to complete the aforementioned legislation, the EBA is now updating the Guidelines issued by its predecessor to establish one common framework for the outsourcing of the financial institutions within the scope of EBA's action.

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

The Guidelines aim to clarify the supervisory expectations regarding the outsourcing to service providers and particular services providers located in third countries in order to ensure that outsourcing is not perform to an extent that would lead to the setting up of empty shells that have not any longer the substance to remain authorised.

The guidelines aim at ensuring that competent authorities are able to identify concentrations of outsourcing arrangements at service providers based on documentation to be provided by institutions and payment institutions in order to reduce risks to the stability of the financial system.

C. Baseline scenario

Outsourcing provisions are currently specified in the CEBS Guidelines on outsourcing. The EBA has published in addition a recommendation on outsourcing to cloud service providers. Outsourcing by firms performing investment services is regulated under Directive 2014/65/EU (MiFID) and Commission delegated Regulation (EU) 2017/565. Outsourcing by payment institutions is regulated within Directive 2015/2366/EU (PSD 2).

Institutions should comply with Directive 2013/36/EU. Article 74 of Directive 2013/36/EU 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 mechanism. The EBA Guidelines on internal Governance specify to a good part the respective requirements, including the need for institutions to have appropriate outsourcing policies (section 8 of the GL), in addition outsourcing needs to be approved as part of the institutions new product approval and change processes (section 18 of the GL).

Article 76 of Directive 2013/36/EU sets out requirements for the involvement of the management body in risk management and Article 88 of Directive 2013/36/EU sets out the responsibilities of the management body regarding governance arrangements that include in both cases outsourced activities.

According to Article 11 of Directive 2015/2366/EU, 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 shall 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 General Data Protection Regulation (EU) 2016/679.

All the above forms the baseline scenario of the impact assessment, which focusses 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) subject to Directive 2013/36/EU (CRD), payment institutions subject to directive 2015/2366/EU (PSD2) and electronic money institutions subject to Directive 2009/110/EC (both referred to as "payment institutions").

Firms providing investment services are subject to the specific provisions on outsourcing included in Directive 2014/65/EU (MiFID II) and EU Commission delegated Regulation 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council.

MiFID 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 lead to inconsistencies between the different frameworks and that there is not a level playing field between investment firms, payment institutions, e-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 CRD, but also payment and e-money institutions. While the guidelines cover all those institutions and payment institutions, the guidelines would not be directly addressed to account information services providers registered only for this service, credit intermediaries and non-bank creditors. Outsourcing arrangements between institutions, 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 under Option B, if the requirements are aligned with the provisions within MiFID and PSD2, would establish a level playing field between different types of financial institutions and ensure that credit institutions can implement one framework for all their outsourcing activities governed by different Directives.

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 6 month and foreseeing transitional arrangements to ensure that institutions can update the assessment of the criticality or importance of outsourcing and update the respective documentation in line with the requirements.

B1) Setting a fixed transitional period of 2 years.

B2) Setting a period of two years (other than outsourcing arrangements to cloud services providers), but requiring to update the documentation if existing outsourcing arrangements are renewed during that period.

All options would be effective to achieve the desired prudential outcome to have all outsourcing arrangements documented in a way that 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 might therefore increase the implementation costs. Therefore Option A has not been retained.

Option B1 and B2 would both ensure that institutions and payment institutions have sufficient time to update their assessments and documentation. Option B2 would lead to a faster update compared to option B1, 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 timeframe for the development of a database that could hold the register. However, for this task the regular implementation period should be sufficient. In terms of cost no difference between option B1 and B2 exists.

Option B2 has been retained.

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

Option A: Relying on the definition provided in MiFID and the Commission delegated regulation and the approach to set more detailed requirements for the outsourcing of critical and important functions.

Option B: As option A, but setting also 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 their activities and develop a good understanding of the scope of outsourcing. A focus on outsourcing of critical or important functions should reduce the administrative costs for 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. Introducing retroactively safeguards for the outsourcing of critical or important function, 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.

Under Option B the framework described under A would apply, in addition some requirements for all outsourcing would be imposed. Anyway for other outsourcing arrangements institutions would need to apply sound processes and document the arrangements, having guidelines 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, but on the other hand, it would be ensured that the process would be subject to additional controls, which should mitigate the additional measures that would need to be taken, if an

outsourcing arrangement becomes critical or important over time, e.g. because of the scalability of the arrangement.

A more narrow definition of outsourcing (option C) for banking activities would limit the number of outsourcing arrangements and this would on first sight reduce the administrative costs for applying the guidelines. However, the framework should ensure a sufficient focus on the outsourcing of critical or important functions and limits by doing so the administrative burden. A different definition would require different frameworks for different activities (e.g. banking vs investment services) and 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) Specify basic requirements on governance arrangements, outsourcing policy, conflicts of interest, business continuity, internal audit function that are in principal covered already in the EBA Guidelines on internal governance

Option A: The guidelines should not specify further 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.

Those Guidelines on internal governance do not apply to payment institutions, hence such an approach (Option A) would be less effective, even if one would take into account that the prudential risks within such institutions would be low compared to institutions that are subject to the CRD.

The inclusion of the listed aspects (Option B) provides certainty for payment institutions regarding the supervisory expectations and ensure respective safeguards within institutions not covered by the CRD. This is desirable also because of consumer protection aspects (e.g. the continuous functioning of payment services should be ensured). For institutions the specifications provided should lead to a higher level of clarity of supervisor expectations and thereby legal certainty.

Option B has been retained.

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

A documentation should be comprehensive, provide an appropriate overview on outsourcing arrangements, including the identified risks of outsourcing of critical and important functions and allow for the identification of concentration risks, by institutions, payment institutions and 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.

B1) Limiting the register only to the outsourcing of critical and important functions arrangements.

B2) Having all outsourcing arrangements documented in the register, but differentiating the extent of documentation between critical or important and other outsourcing.

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

Option D: In addition to require a register, a requirement to inform in a timely manner competent authorities about all new the outsourcing of critical and important function could be set.

Option E: As option D, but a prior approval or non-objection procedure by the competent authority would be required.

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

Option B would ensure that institutions, payment institutions and competent authorities have an overview on all relevant outsourcing arrangements and would be in a position to assess risk concentration. The definition of a minimum set of aspects to be documented 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. Including at least a limited set of information (Option B2) for all other outsourcing would facilitate even better the identification of concentration risks. As a register would already exist, the costs would be low as they would be limited to the input of a few additional data into the register. Option B2 would be more efficient then Option B1.

Adding also 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 cost for adding such arrangements to the register. However, if only nearly certain arrangements are entered into the register, this would usually happen in a short time frame and hence such a process might not ensure that competent authorities are informed in a timely manner about upcoming outsourcing arrangements.

Option D would ensure that competent authorities would be informed about upcoming outsourcing arrangements and have the opportunity to intervene if they had concerns about the risk they encounter or if such an arrangement would lead to a situation where the institution would become an empty shall that lacks the substance for its ongoing authorisation. Such an information would

lead to a low cost impact for institutions and payment institutions, but if a feedback of the competent authority (Option E) would be expected this might delay the implementation of arrangements and could therefore lead to additional cost.

Option B2 and D have been retained.

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

Option A: The guidelines could leave it open for institutions and payment institutions to develop their own assessment framework.

Option B: The guidelines could specify in line with MiFID and PSD2 requirements the approach to assess 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 one harmonised framework which takes into account the assessment criteria provided in a MiFID and PSD context, but would provide additional criteria for the assessment of the impact of outsourcing arrangements. An assessment of the operational risk impact is one aspect that is relevant for the decision if an outsourced function would be critical or important. Such risks include also the so-called step in risk that may be triggered if the service provider would be in financial distress and would need financial support by the institution and payment institutions to maintain the services towards the institution. A harmonised set of criteria to be implemented by institutions and payment institutions would not create more costs as compared to institutions defining their own framework. However, where there is already a framework in place in line with the MiFID and PSD requirements institutions would have one off costs for adjusting that framework.

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

Option B and C have been retained.

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

Although most outsourcing arrangements involve activities or services (or parts thereof) which 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 that are directly subject to authorisation in their Member State to service providers located in third countries. The outsourcing of investment services is regulated under Commission delegated Regulation 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 applies, outsourcing to third countries would in most cases not be subject to the same framework. Therefore, this specific type of outsourcing arrangement should only be allowed if:

- the service provider in the third country is authorised by a relevant supervisory authority to perform the activity or service; and
- the outsourcing 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 the competent authority being able to receive the information needed for its supervisory tasks, exercise access and audit rights in the third country and the existence of mechanisms for the exchange of information on enforcement matters.

Two policy options have been considered.

Option A would only allow the outsourcing of banking and payment activities or services, that are subject to authorisation or registration, to third countries, 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 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 step in, if effective supervision would not be 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 case of outsourcing of functions of portfolio management and ensure that the respective 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 it belongs to institutions and payment institutions to ensure that there is a copperation agreement between their competent authoritity and the competent authority of the third country where they

outsource those banking and payment activities or services If a cooperation agrrement does not exist, then outsourcing of banking and payment activities or services in the third country is not possible.

Option B recognised 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 assess that they can effectively discharge their supervisory duties in practice. In particular they 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 it concerns an activity or service that is itself subject to authorisation if they were not satisfied that they will be able to effectively supervise it.

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 reflect at least the required documentation requirements.

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

Option B: The guidelines 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 that the institution and payment institution are responsible for their outsourcing arrangements. Requirements specified in a Mifid and PSD context 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 etc).

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 particular 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, their implementation for other new outsourcing arrangements should not lead to material additional cost, but 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 respective supervisory processes for payment institutions.

Option A: The guidelines should provide for a detailed procedural framework for the 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 leave the detailed setting of 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 EBA guidelines. For payment institutions competent authorities are in any case be informed about outsourcing of payment services. However, given the periodically of the SREP, additional information on new critical or important outsourcing, while carrying a low additional costs, ensure 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 specify requirements on institutions, payment institutions and competent authorities under the already existing framework that provide mainly clarification and procedural guidance.

A higher level of clarity on outsourcing benefits institutions by creating a higher level of transparency of regulatory requirements. Standardised requirements lead to a reduction of 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 to input 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 aims at ensuring 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 and payment institutions, which will differ depending on the nature:

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

b. For CRD-credit institutions a detailed framework exists regarding their investment and payment services and activities, regarding their banking activities the previous CEBS guidelines applied, hence the additional costs triggered by the guidelines should overall be low.

For institutions and payment institutions the guidelines may create low additional costs for additional documentation requirements and the implementation of a register (e.g. in form of an database). Some minor one off costs may be triggered by the need to update outsourcing policies and costs for establishing and maintaining the register of all outsourcing arrangements (e.g. in terms of additional data input on top of existing documentations). The overall impact is considered low, as institutions and payment institutions must in any case have documentation in place on their organisational structure, which includes outsourcing arrangements. On the other hand, a register will create benefits for the management of outsourcing arrangements.

There are low additional costs, as the assessment of the criticality or importance of outsourcing arrangements by CRD-credit institutions is required based on harmonised criteria which need to be implemented by institutions. However, institutions and payment institutions should have such processes in place regarding their investment and payment services and activities. Therefore the additional costs should be very low off costs for implementation of procedures. Given existing procedures, the cost for applying new procedures should be minor.

There are low additional costs for institutions and payment institutions within the risk assessment of outsourcing arrangement as a more thorough assessment of the operational risks and step-in risks are required. All institutions and payment institutions should however already be familiar with risk assessments and the conduct of scenario analysis and perform such risk assessments.

Clear contractual requirements, including requirements to assure access and audit rights lead to minor one off costs for their implementation, they reduce however 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 specification of how audits can be performed is based on already existing recommendations and therefore does not trigger any additional costs.

Q16: Are the findings and conclusions of the impact assessments appropriate and correct; where you would see additional burden, in particular financial costs, please provide a description of the burden and to the extent possible an estimate of the cost to implement the guidelines, differentiating one-off and ongoing costs and the cost drivers (e.g. human resources, IT, administrative costs, etc.)?

5.2 Overview of questions for consultation

Q1: Are the guidelines regarding the subject matter, scope, including the application of the guidelines to electronic money institutions and payment institutions, definitions and implementation appropriate and sufficiently clear?

Q2: Are the guidelines regarding Title I appropriate and sufficiently clear?

Q3: Are the guidelines in Title II and, in particular, the safeguards ensuring that competent authorities are able to effectively supervise activities and services of institutions and payment institutions that require authorisation or registration (i.e. the activities listed in Annex I of Directive 2013/36/EU and the payment services listed in Annex I of Directive (EU) 2366/2015) appropriate and sufficiently clear or should additional safeguards be introduced??

Q4: Are the guidelines in Section 4 regarding the outsourcing policy appropriate and sufficiently clear?

Q5: Are the guidelines in Sections 5-7 of Title III appropriate and sufficiently clear?

Q6: Are the guidelines in Sections 8 regarding the documentation requirements appropriate and sufficiently clear?

Q7: Are the guidelines in Sections 9.1 regarding the assessment of criticality or importance of functions appropriate and sufficiently clear?

Q8: Are the guidelines in Section 9.2 regarding the due diligence process appropriate and sufficiently clear?

Q9: Are the guidelines in Section 9.3 regarding the risk assessment appropriate and sufficiently clear?

Q10: Are the guidelines in Section 10 regarding the contractual phase appropriate and sufficiently clear; do the proposals relating to the exercise of access and audit rights give rise to any potential significant legal or practical challenges for institutions and payment institutions?

Q11: Are the guidelines in Section 11 regarding the oversight on outsourcing arrangements appropriate and sufficiently clear?

Q12: Are the guidelines in sections 12 regarding exit strategies appropriate and sufficiently clear?

Q13: Are the guidelines in Section 13 appropriate and sufficiently clear, Iin particular, are there any ways of limiting the information in the register which institutions and payment institutions are required to provide to competent authorities to make it more proportionate and, relevant? With a view to bring sufficient proportionality, the EBA will consider the supervisory relevance and value of a register covering all outsourcing arrangements within each SREP cycle or at least every 3 years in regard of the operational and administrative burden.

Q14: Are the guidelines for competent authorities in Title V appropriate and sufficiently clear?

Q15: Is the template in Annex I appropriate and sufficiently clear?

Q16: Are the findings and conclusions of the impact assessments appropriate and correct; where you would see additional burden, in particular financial costs, please provide a description of the burden and to the extent possible an estimate of the cost to implement the guidelines,

differentiating one-off and ongoing costs and the cost drivers (e.g. human resources, IT, administrative costs, etc.)?