Comments

on EBA Draft Guidelines on Outsourcing Arrangements (EBA/CP/2018/11)

Our ref

Ref. DK: EBA-GL

Ref. DSGV: 7205/05

GBIC Transparency Register ID: 52646912360-95

Contact: Christina Pfaff

Telephone: +49 30 20225- 5427

Fax: +49 30 20225 5404

E-mail: Christina.Pfaff@dsgv.de

Berlin, September 24, 2018

Coordinator:
German Savings Banks Association
Charlottenstrasse 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Fax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

1. General Comments

Consistent guidelines are useful for creating a level playing field, not least because the existing 2006 CEBS guidelines were implemented in different ways by the EU member states. Nevertheless, both the institutions and the supervisors should retain some leeway so as to take due account of the principle of proportionality and the specificities of the national banking sectors.

Unfortunately, it is the case that the scope of regulation of the present draft guidelines has risen by a factor of ten compared with the existing CEBS guidelines. Overall, the outsourcing requirements are too detailed. The disclosures stipulated by the ECB's draft regulation are considerably more extensive compared with the national requirements. As an example, the German MaRisk (Minimum Requirements for Risk Management) contain eight requirements for outsourcing arrangements, whereas the Draft EBA guidelines contain 26 requirements (paragraphs 62 et seqq.). The requirements for legal analysis (paragraphs 61 et seqq.), the tests of exit strategies (paragraphs 89 et seqq.) and the notifications to the supervisors (paragraphs 92 et seqq.)] are also too far-reaching. The GBIC wishes to point out that more regulation is not necessarily better regulation, and therefore urges streamlining the proposals overall.

The outsourcing solutions used by the institutions are highly tailored to the individual institution in many areas. In an era of digitalisation and the growing importance of information technology, the institutions will need to outsource certain activities and processes to an even greater extent in the future. In light of this, we believe that principle-based regulatory requirements in the area of outsourcing are appropriate and reasonable. We see a risk that too heavily rule-based requirements will rob the institutions of the flexibility and efficiency they need in connection with outsourcing to third parties. A possible consequence would be that the institutions would lose cost advantages because of the regulatory requirements, or that they would no longer be able to use external expertise, even though this makes sense from a risk perspective.

In light of this, we believe that the current definition of outsourcing (that is based on MiFID II but does not feature the restrictions also provided for in MiFID II) is too broad, and that a narrower definition of outsourcing is therefore needed. As a general principle, the question of which requirements apply to which outsourcing scenarios is not sufficiently clear in the guidelines.

In the "banking" context, the current definition is far too broadly worded and would cover a range of services that are not directly related to the banking business, but would still be classified as outsourcing. It should therefore be clearly emphasised that the requirements only have to be applied if the outsourced activities relate to the banking business or are essential for supporting the performance of banking business processes. On the other hand, there needs to be a clearer distinction between the requirements for outsourcing of critical and important functions and those for non-critical/non-important functions. Expanding the requirements to any transfer of activities to third parties, regardless of their importance for performing banking business, would firstly lead to a massive expansion of administrative effort for the affected institutions and violate the principle of proportionality. Secondly, many of the service providers who offer such business-neutral activities mainly to companies outside the financial sector would not be in a position to meet the requirements for e.g. internal audit and reporting.

This also applies in particular to non-critical and non-important outsourcing arrangements in which the institutions should have far-reaching freedom with regard to designing a proper governance system.

It should therefore be clarified that the requirements apply only to activities related to banking and to critical or important outsourcing activities. As a minimum, it should be clear which of the requirements in

the guideline apply only to the outsourcing of critical or important functions. In this case, we believe that it is vital to significantly reduce the requirements for non-critical outsourcing arrangements. To enable a better definition, the EBA should also provide a non-exhaustive list of activities that are not considered to be outsourcing or outsourcing of critical or important functions within the meaning of the guidelines.

In addition, we believe that the list of services in paragraph 23 and the examples in Annex 1 are, in part, contradictory. Moreover, the requirements e.g. for risk assessments in paragraph 57 have even been extended beyond the definition of outsourcing to other purchased services, which we believe goes far beyond the scope of these guidelines. More detailed remarks on this issue can be found in the comments on the individual questions and paragraphs.

The permanent divisions of responsibility within groups and financial networks belonging to IPSs should be appropriately taken into consideration.

In the case of groups, the centralised risk management for the entire group required there under EU law should also be considered to be risk-reducing. Intra group outsourcing should be subject to lower compliance and reporting obligations than third party outsourcing arrangements. Guidelines should recognize the degree of integration reached within many banking groups, where centralised functions at group level act as a service provider for the other entities of the group. In this context, the proposed requirements on documentation, due diligence, concentration risk and exit strategies prove to be less relevant or even irrelevant from an intra group perspective.

Outsourcing to specialised service providers also always brings advantages such as risk reduction, quality improvements or sharing in innovations. Using them may not be effectively prohibited because of excessive regulation and an unreasonably high effort for the institutions, which can be identified by duplication of effort for control and audit activities at the insourcer and the outsourcer, in particular if the service provider is a regulated entity. Specifically:

- Risk analysis and control activities by the outsourcing institution that relate to matters that are already supervised by the competent authority responsible for the service provider or that are the subject of a mandatory supervisory or voluntary external audit (e.g. organisational precautions, in particular risk management)

- Option for the outsourcing institution to refer to the external audit report of the outsourcer acting as a multi-client service provider instead of its own control activities, to the extent that the services provided to the outsourcing institution are the subject of that audit.

We urgently request that the national specificities, many of which have evolved historically over a long time, are sufficiently taken into account. The responsible supervisors should have a sufficient margin of discretion for their assessment and treatment. This also applies to cases in which a specialised service provider has not (or no longer) assumed certain activities (such as principal broking services or safe custody business) only for institutions in a group of institutions, but equally for institutions in different groups of institutions. This is the case in particular if banking services can be offered by small and medium-sized institutions only if certain activities are outsourced to a specialised infrastructure services provider (“centralised service providers”) that works for a range of banks because of the high level of technology involved and/or the complexity of their regulation.

It should also be clarified that no prior approval by the NCA and also no notification to the NCA are necessary for an outsourcing arrangement.

Moreover, we wish to point out that forcing service providers to accept the requirements may prove to be a problem if a service provider does not wish to accept them. It is perfectly possible that outsourcing relationships that were “inconspicuous” in the past – in the sense that they were managed commensurate with the risk – are affected by this. We do not assume that there is an expectation that such contracts will have to be terminated and replaced by service providers who may meet the supervisory requirements, but for which there are concerns about their ability to perform the service to the required level of quality. It is therefore doubtful in the context of IT outsourcing whether large international companies (Microsoft, SAP, etc.) can be controlled by means of banking regulation via the individual banks. On the contrary, too strict regulation could disadvantage small fintechs and hinder cooperation and innovation. In addition, we believe that the supervisors themselves are responsible for monitoring large infrastructure/cloud providers for the financial markets. The banks remain responsible for appropriately managing the service relationships. The NCAs should be required to take over relevant requirements for standards or to safeguard the financial market infrastructure.

Standard contractual clauses are necessary for outsourcing agreements: Financial institutions may find it difficult to negotiate some of the terms required by these guidelines and persuade some large suppliers to accept them, such as the exercise of unrestricted access rights, or ex ante notification and pre-approval requirements for sub-outsourcing. Meeting documentation requirements (e.g. regarding sub-service providers) will also depend on the willingness of third parties to provide the information. Standard contractual clauses would be required for the supplier negotiation process. In this respect, we welcome the European Commission's work in the context of cloud service providers, and believe that it would be positive in other contexts as well.

2. Specific Comments

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?

Paragraph 11

The exclusions given in paragraph 23 are relevant for the definition of outsourcing and should be relocated to paragraph 11. As a general principle, only the acquisition of services relating to the supervised activities should be regarded as outsourcing within the meaning of the guidelines. In addition to the services, goods and utilities given in paragraph 23, there are additional functions (for example personnel administration) for which the application of the comprehensive requirements would be inappropriate.

Additionally, the acquisition of non-recurring and occasional services should be excluded from the application of the requirements.

The definition of outsourcing is too broad. National requirements are based on typical bank or institution activities and processes that are regularly outsourced. We therefore propose the following definition: “*Outsourcing means an arrangement of any form between an institution and a service provider by which that service provider performs a recurring (transactional) process, a permanent service or a regular activity in close connection with performing banking or investment activities of the institution which would otherwise be undertaken by the institution itself according to its respective business model (services which are related to banking/CRR business). This includes the outsourcing of systems and functions and parts of the aforementioned supporting core banking business processes.*”

According to the definitions, a critical or important function includes any operational tasks performed by the internal control functions. We understand that outsourced functions that are not significant are deemed not to be critical outsourcing arrangements, even when they support control functions (e.g. supporting activities such as data preparation for internal controls).

Only a few examples are listed in the draft EBA guidelines and some more guidance would be very helpful, especially with regard to examples that should not be seen as outsourcing. A (non-exhaustive) list of negative examples would certainly be helpful here.

Given the fact that the EBA refers to the MiFID II-definition of "critical or important functions" (see also paragraph 5 of the Draft guidelines): will the guidelines be expressly updated/amended by the EBA in the event of modifying interpretations by ESMA as the competent MiFID authority, e.g. by way of ESMA Q&A, or will ESMA statements (Q&A) on MiFID II outsourcing automatically apply to the guidelines, with the result that institutions must constantly monitor ESMA Q&A developments and their implication for the guidelines? We are of the opinion that only the answers given by the EBA should apply to all outsourcing arrangements that comprise activities beyond the scope of MIFID II.

Based on the different directives and regulations (CRD IV, PSD II, eMoney Directive, CRR, EBA guidelines on internal governance), with their possibly diverging definitions referred to in the Definitions section, the EBA should clarify that only the regulation directly applicable to the activities of the relevant institution applies (alternatively/additionally, a complete cross-reference/concordance list with all relevant definitions as an Annex to the guidelines would be useful) (see paragraph 11 of the GL);

Please also note that the wording in the Outsourcing definition under paragraph 11 deviates from the one used in paragraph 23 of the Draft guidelines.

Regarding the definition of sub-outsourcing: "… considered as an outsourcing to another service provider … The definition should specify that it refers solely to tasks that were initially transferred in an outsourcing arrangement (excluding any sub-supply that would not be considered as outsourcing by a bank)

Regarding the definition of cloud services: The addendum "meaning ICT services…" within the definition of cloud services would restrict the services to ICT-related outsourcings. For business process outsourcing arrangements, the topics of related data etc. should be addressed in the same way as any other ICT platform being used. The requirements later on related to cloud are ICT specific and therefore should not include in any contract just because some of the components at the provider or any sub-provider could be in a cloud environment.

Paragraph 12

The GBIC welcomes the option for phased implementation of the guidelines. However, we believe that it is urgent for initial application to be postponed to 1 January 2020 at the earliest. The Draft guidelines contain extensive requirements. Experience shows that it takes some time for the EBA to obtain translations of the final guidelines and for the competent authorities to publish their statements. The institutions must then be given sufficient time for implementation.

The question of what is expected for long-term contracts should be clarified: paragraph 12 expects them to be made compliant with the guidelines at the next renewal date (which could be in 5 to 10 years), whereas paragraph 13 expects to have the register completed by the end of 2020, which then possibly results in missing information because the contract has not been renewed (e.g. all details on sub-outsourcing).

Paragraph 13

We wish to point out that amending an existing contract entails substantial economic risks. It is conceivable for the new specifications for the outsourcing agreements to be adopted when the contract expires. We wish to propose a risk evaluation for the residual term of the contract.

Regarding the scope: The outsourcing definition is not clear enough as it does not specify any element for guiding the assessment of the scope of the outsourcing. Those elements should be: contents of the activity provided by the third party and the related duration and frequency (please refer to the amendment proposed for point 17 of the chapter “Rationale and objective of the guidelines”). In the particular case of outsourcing to the cloud, these guidelines should provide a clearer definition of the type of cloud (Shared, Dedicated, Public, Cloud and Private Cloud) and the type of service (IaaS, PaaS, SaaS …). Outsourcing to cloud service providers should only be considered as such when it affects critical functions.

In order to provide clarity on what the specific requirements for each type of outsourcing are, it would be helpful to compile them all in a specific table or diagram to identify which are applicable to each service. In addition, given the particularities of outsourcing to cloud services and given that the EBA recommendations on cloud outsourcing will be repealed when these guidelines enter into force, it would be necessary to include a section with all specific requirements for cloud computing.

Concerning the definition of sub-outsourcing, we believe that such cases in which the main service provider delegates part of the service or contracts any good, tool or license to a third party should not be considered sub-outsourcing, provided that such delegation or contract does not represent a significant part of the critical service supplied as a whole by the service provider. Institutions should consequently be discharged from their obligations regarding such sub-outsourcing situations due to the complexity of overseeing them in practice.

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

As expressed under “Rationale and objective” (paragraph 26), the EBA is of the opinion that intra group outsourcing is not necessarily less risky than outsourcing to an entity outside the group. In light of this, the EBA proposes that intra group outsourcing should be subject to the same legal conditions as outsourcing to service providers outside the group. We believe that a distinction is generally justified, but wish to point out again in this context that functionally equivalent arrangements may also exist if the service provider is integrated into several groups of institutions (supervised multi-client service provider).

This is particularly the case if the outsourcing involves a parent entity and a subsidiary, the parent holds the majority of the voting rights and equity interests, and both entities are subject to banking supervision. In such cases, the parent entity not only bears an economic risk, but also has a vested interest in ensuring the uninterrupted operation of all processes and systems, including at the subsidiary. As the superordinate entity, the parent entity is normally responsible for compliance with prudential requirements at group level and is legally obliged in this connection to establish appropriate risk management and control processes that also include the subsidiaries. In light of this, we believe that the potential conflicts of interest addressed in the EBA guidelines do not exist or are extremely limited if a subsidiary outsources to the parent entity. We therefore suggest making a distinction with regard to the outsourcing requirements in the case of intra group outsourcing, and additionally to create exemptions for comparable cases of supervised multi-client service providers.

Paragraphs 17 and 18

Please further specify what kind of subsidiaries are subject to these requirements. All subsidiaries regardless of their status (e.g. only with banking licenses, subsidiaries considered as material from a group perspective)?

Paragraphs 19 and 20

The GBIC welcomes the fact that risk-based waivers and accordingly facilitations will be available for outsourcing within groups and institutional protection schemes (IPS). We believe that this is generally justified because such groups and groupings are focused on long-term cooperation and a rational division of responsibilities. However, the requirements in the outsourcing guidelines should be broken down further and supplemented.
The governance and ownership structures in an IPS can be different to those of a consolidated group within the meaning of Article 11 et seqq. of the CRR (Regulation (EU) 575/2013). Based on paragraph 35c) of the Draft guidelines, we are requesting that, for an IPS, all outsourcing to other entities affiliated with the corresponding financial network and supervised multi-client service providers should be covered, as well as outsourcing arrangements between the member institutions.
In addition to the options given in paragraph 20, the inclusion of further exemptions for groups is appropriate. These are addressed in our comments on the relevant paragraphs.

In the absence of any waiver granted under the CRR or the CRD, the guidelines apply at group consolidated level and at solo level (i.e. the subsidiaries of a cross-border group must fulfil the requirements). We believe that the parent entity should have management mechanisms in place for its subsidiaries to ensure compliance with the guidelines, although responsibility should lie with the subsidiary and not both entities.

Paragraph 19

Subparagraph b): It may provide more clarity if this subparagraph is amended as follows:
"*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.*"

Reasoning: Competent authorities cannot obtain "their" individual register, it is the register of the institution. Also, there is no basis for regulating the relationship between non-EU subsidiaries and their non-EU supervisory authorities.

Please clarify this in order to achieve a better understanding of the Outsourcing definition: If such a register is applied centrally, is it then considered to be the outsourcing of a critical or important function according to paragraph 49 a) (i), as it would be considered to be a regulatory requirement for the institution to provide such a register?

Subparagraph c): Please delete "*within the group*" as it might be necessary to outsource parts of the control function tasks to external parties, e.g. audits for which technical expertise is necessary (e.g. ICT tasks) or when there is an intention to "join forces", e.g. in pooled audits as proposed in paragraph 8 a) of the "EBA Recommendations on outsourcing to cloud providers".

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?

Paragraphs 22 and 23

In accordance with paragraph 22, the institutions should assess whether an arrangement with a third party falls under the definition of outsourcing. Paragraph 23 clarifies that the acquisition of services, goods or utilities that are not normally performed by the institutions themselves is not considered to be outsourcing. In the context of the definition of outsourcing, we propose that services that are provided using cloud computing and that are acquired by the institution should not be classified globally as outsourcing. The content that is stored in a cloud should be considered. Issues that are not relevant for outsourcing purposes (e.g. software for canteen plans, media portal) should not be classified globally as outsourcing and hence overregulated simply because they happen in the cloud. We therefore suggest narrowing the specification of the content that is stored in the cloud.

We believe that there is currently still room for interpretation with regard to the treatment of software and maintenance agreements. Such agreements are not explicitly mentioned, as a result of which it is not clear whether they have to be treated as outsourcing. We suggest providing defined examples to ensure clarification in the same way as telephone lines are given in paragraph 23.

Paragraph 22

The wording of the second sentence in this paragraph goes too far. Any form of cooperation amongst licensed entities would have to be qualified as “outsourcing”. However, there are, for example, functions of central clearing houses in payments or securities settlement that can definitely not be performed by individual institutions and should thus not be considered to be outsourcing within the meaning of the guidelines. We suspect that the intention behind this requirement is in particular to ensure that there cannot be any reference to capacity or expertise that an institution currently does not possess. This could be better expressed as follows:
“*it is not relevant whether or not … or it would be able to perform it by itself on the basis of current resources and capabilities.*”

The last sentence is an element of the definition of outsourcing, and should thus be added under paragraph 11.

Paragraph 23

In our understanding, any form of one-off purchase of goods or services should not qualify as outsourcing, as well as any form of pure advice (e.g. legal, tax, marketing advice, management consulting etc.), it being understood that the decision on how to deal with the advice provided (and what actions will be taken) always remains with the institution.

Is our understanding correct that the reference to activities “normally” performed by the institution is restricted to such banking activities it is licensed to perform?

The term “services” is rather indistinct as it is not fully clear how this really differs from some subcategories mentioned in Annex 1 (e.g. Participation management would be not connected to banking services, it

is part of executing institutions owner rights). Therefore, we are requesting clarification of which subcategories are defined as outsourcing and which are not.

Paragraph 24

The GBIC opposes a requirement to perform a risk assessment in accordance with section 9.3 of the Draft guidelines, among other things, for all of an institution's contractual relationships. The analyses and assessments required there are likely to be excessive for almost all other contractual relationships, and this is not something that can be remedied by a general reference to the principle of proportionality. The requirement for other contractual relationships should be limited to their inclusion in the management of operational risk and ensuring compliance with the legal provisions to be observed by the institution.

We believe that applying paragraph 24 to intra group arrangements and services provided internally between functions within the same legal entity would create an extra burden just because of the internal business model of each institution (as described in Q1). Risks will not be reduced just by insourcing a function, but according to current guidelines it seems that if an institution can internalise, there is no need to apply the mitigation risks indicated in paragraph 24.

Paragraph 26

This requirement states that, for example, a function may only outsourced to a service provider in Singapore if MAS has an agreement with the EBA that fulfils certain conditions. How are the institutions supposed to know that? In our view, this requires the disclosure of the agreement between EBA and the supervisory authority in the third country. The NCAs should publish a list of the countries with which they have such agreements, covering explicitly the mentioned criteria under paragraph 26(b) and 26(c i – iv). In addition, it should be ensured that institutions are not required to monitor the existence of such MoUs throughout the existence of their outsourcing agreements. In case an NCA terminates a MoU with another NCA, it should be required to inform the supervised institutions. In addition, the EBA should provide transitional periods in the event that the negotiations on a MoU between NCAs are still ongoing.

In the case of outsourcing to cloud service providers, it is important to make a distinction between Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Background: IaaS is not specific in relation to the customised service/product the bank offers in its business model or uses for its business operations. In other words, IaaS corresponds to the infrastructure a bank uses, for example when it needs a footpath or road so that customers can reach the bank, or needs a building in which the bank can run its business. SaaS is then the customised component that can be – but does not have to be – outsourced. IaaS can therefore be acquired from a third party, for example (not outsourced). The software that runs on the infrastructure or platform is managed internally by the institution (not outsourced). Only if the software is operated as SaaS is there an outsourcing arrangement for (only) the SaaS.

Generally, there should be less restrictive requirements in the case of outsourcing to an own subsidiary (or a parent company) in a non-EU country.

Paragraph 26a)

Under the basic rule that the "institution remains responsible for the service", why is it necessary for the provider is properly supervised by an NCA? If no controls can be eliminated by choosing a supervised provider, there will be duplication of effort in the system. We therefore propose removing this clause. If it is kept:

- is our understanding correct that it is sufficient for the service provider to be allowed to perform the outsourced activities (in line with paragraph 25 b)) in case there is no authorisation requirement under local law?
- Institutions are not in a position to decide on the question of "effective supervision", so further guidance by the EBA is required here.
- As this clause is dependent on judgement outside the institution's sphere of influence: is there any automatic obligation to terminate such agreements if the NCA considers formerly sufficient supervision not to be sufficient, or is a formal process according to paragraph 105 to be applied?

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

Paragraph 28e)

In the view of the GBIC, the term "day to day management" used here appears to be inappropriate with regard to the responsibilities of the management body. In accordance with the governance guidelines, senior management underneath the management body is responsible for operational management of an institution. It also would be an exaggeration to make the management body responsible for the full details of managing the risks associated with outsourcing arrangements.

Paragraph 32

We propose revising this sentence as follows: "*When outsourcing, institutions and payment institutions should ensure, considering the principle of proportionality, that:*"

NCAs should consider that the principle of proportionality might be applied when setting up contracts and governance, as e.g. sub-outsourcing in paragraph 62d is applicable only to outsourcing of critical or important functions.

Subparagraph e): If there are any risks specific to fintech, they should be mentioned or otherwise the term "fintech" should be excluded, as in principle all technological developments have to be considered regardless their source or origin.

Subparagraph h): The sentence "…and data is stored and processed in accordance with Regulation 2016/679." should be deleted as this already extensively addressed in the GDPR; additionally, there is data that is not subject to the GDPR in foreign subsidiaries, where this rule might conflict with local law.

Proportionality considerations must also apply in special national scenarios, for example if a service is outsourced to a regulated centralised service provider.

Subparagraph d) proposes that internal control functions should have sufficient rights, resources and access to the management body of the service provider to perform their tasks. It should be sufficient for audit findings of internal or external auditors of the service provider to be available.

Paragraph 33 – Editorial note: Section 8 (rather than 4) of the Governance guidelines

Paragraphs 33 et seqq.

We would urge the EBA to clarify that the application of the guidelines on sub-consolidated and consolidated basis is restricted to consolidated entities to which the statutory outsourcing provisions are "applicable" only (see also paragraph 9 etc. of the guidelines); otherwise the statutory scope of application would go far beyond statutory regulation (e.g. section 25b(1) of the German Banking Act).

Paragraph 34

Subparagraph c) point ii: We suggest revising this sentence as follows: *"… (e.g. to its financial position, organisational structures relating to the functions outsourced or ownership structures, sub-outsourcing)."*

Organisational structures should only be reported to the extent relevant for the provision of the outsourced services.

Subparagraph e) point i: should be applicable also only to critical or important functions, as they deemed relevant for the company. Other outsourced services could be managed using generic plans to be detailed on ad hoc base.

Subparagraph e) point ii: We suggest a revision as follows: *"…for each external critical…"* as intra group providers are subject to a variety of BCM/DR/recovery and resolution planning procedures and additional planning/documentation is not necessary.

Paragraph 35

Further clarification would be required regarding what is meant by "providers which are authorized by a competent authority" and which are the frameworks that support this authorisation.

Paragraph 35c)

The term "intra group outsourcing arrangements": it is unclear whether outsourcing of activities by an institution (e.g. subsidiary in a banking group) to a service provider (e.g. other subsidiary in a banking group) which is member of the same banking group, but not controlled by the outsourcing institution itself, qualifies as "intra group outsourcing" arrangement and will be administered/managed in the same way. For example, paragraph 19 (a) refers to "outsourcing arrangements with service providers within the group or ….", paragraph 47 b) iv) refers to the "institution's group" and 48 (f) sets out that the institutions must consider considered whether the service provider is part of the "institution's accounting consolidation group". These definitions differ slightly and therefore leave room for interpretation whether outsourcing as described above (to a service provider not controlled by the outsourcing institution but member of the group the institution belongs too) is treated in the same way as outsourcing within the "institution's accounting consolidation group".

Paragraph 35d)

It must make a difference whether this relates to an unregulated service provider – possibly outside the EU – or a service provider within the EU/EEA that is subject to in-depth supervision as a CRR institution.

As a consequence, and as a benchmark for the supervisors, exemptions must be provided because – if it is a credit institution – the service provider will in any event be nationally supervised and subject to banking supervision. As a matter of principle, this case must be treated differently to an unsupervised, unregulated service provider in a third country. Duplicate effort for audits (outsourcer and insourcer) can

and must be avoided through this distinction. The scope of the audit in paragraph 42 would thus be reduced.

Paragraph 38

The intention of the final sentence in this paragraph is not clear, and at least no clear connection with the management of conflicts of interest is evident.

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

Section 7

Paragraphs 74 and 75 allow third-party certifications and reports and pooled audits to be used complementary to audits of the institution's internal audit function. These options should also be mentioned in section 7.
In addition, many service providers themselves have an internal audit function that meets national and international professional standards. In this case too, it should be clarified that their audit activities may also be used.
In particular when the service providers are supervised institutions or they work for a large number of clients, inappropriate multiple audits should be avoided. These would not generate any appreciable additional benefits, but rather operational stress and higher costs.

Paragraphs 37–38

Paragraph 37 and paragraph 28c) state that institutions or the management body should identify, assess and manage conflicts of interest with regard to their outsourcing arrangements. Please clarify when a conflict of interest can arise the form that such an assessment of conflicts of interest should take. As already discussed above (paragraph 18), we believe that there are no – or only very limited – such conflicts of interest in the context of intra group outsourcing if the parent entity holds the majority of the voting rights and equity of the subsidiary and both entities are subject to banking supervision.

We believe that a presumption that intra group agreements can be problematic in terms of conflicts of interest – and, based on this, the burden of considering any intra group agreements to be outsourcing – penalises the entities that are organised as subsidiaries, although they may not be taking more risks than others.

Paragraph 42

As the audit right is usually limited to the services provided, this point needs also to be restricted to this perimeter. The audit function of the service recipient cannot cover the entire risk appetite, risk management and control procedure of the service provider. The audits do not necessarily have to take the form of an on-site audit. It is our understanding that it is sufficient for compliance to be confirmed by an internal or external auditor.

Paragraph 43

We would ask the EBA to delete the words "in particular" as this clause specifies audit tasks as demanded in 10.3. From our view, it should be applicable only for critical or important functions. Otherwise, all contracts would require full audit rights, which would mean additional burdens for the institutions to integrate these in each contract, especially for subsidiaries outside the EU, where this is not common.

Paragraph 44

We believe that the internal audit requirements are very far-reaching. We propose making the required information dependent on the risk. The far-reaching information requirements should therefore be limited to critical and important outsourcing activities, with less extensive requirements existing for other outsourcing arrangements.

Paragraph 44d)

Service providers do not have to be institutions and there is therefore no requirement for them to meet dedicated requirements, for example regarding the definition of their risk appetite. If the service provider is an institution, it must itself meet all the governance requirements so the outsourcing institution may not impose any strategic requirements on it. The GBIC proposes revising subparagraph d) as follows: "*the adequacy of the risk management and control procedures of the service provider;*"

Internal audit should concentrate solely on the risk management and control procedures relating to the outsourced activities. In this context, internal audit should examine whether the outsourcing arrangement is appropriate and whether the service provider complies with it. Please clarify that primary responsibility for the service provider's risk appetite, risk management and control procedure lies with the strategy for the first or second line of defence.

Paragraph 45

According to the EBA, all audit recommendations and findings should be subject to a formal follow-up procedure by internal audit. If this means own audit procedures in central outsourcing management, technical/operational outsourcing monitoring, or at the service provider itself, this follow-up happens in practice. This also applies to the findings of the auditor or the institution's supervisory authority. Please clarify that an institution's internal audit function can, in the future, continue to rely on audit activities performed elsewhere (e.g. at the service provider) in certain cases – as provided for under national law in Germany – provided that there is evidence of their proper functioning. The institution's follow-up procedure in the case of deficiencies should therefore not relate to cases in which, for example, the outsourcing provider's internal audit performs the auditing function. In this case, the institution should continue to be able to rely on the service provider's internal audit to rectify the deficiency. Audit recommendations and findings resulting from the audit activities of the service provider are taken into account by the institution/payment institution in the risk assessment of the outsourcing arrangement and followed up at an aggregated level.

We also suggest that there should be a fundamental distinction with regard to risk (proportionality). Follow-up by internal audit should only be required for critical and important outsourcing arrangements.

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

Paragraphs 46 and 47

The EBA proposes that the institutions should maintain a comprehensive register of all outsourcing arrangements. The requirements imposed on the register are extremely detailed and go far beyond the services overviews currently maintained by the institutions, also because paragraph 47 only makes a partial distinction between important and non-important outsourcing arrangements. A banking supervisory benefit is not evident for many requirements and/or meeting the requirement is associated with a high bureaucratic effort for the institutions, e.g.:

- a list of all entities in the group that make use of the outsourcing arrangement (paragraph 47a) point v),
- the date of the last and the next scheduled audit (paragraph 47c) point v),
- continuous assessment of the service provider's substitutability and the possibility of reintegrating the service back into the institution (paragraph 47c) point vi),
- maintaining a list of alternative service providers (paragraph 47c) point vii).

We therefore suggest reviewing the requirements for the scope of the register of outsourcing arrangements.

Paragraph 46

Please specify in more detail what type of subsidiaries should be subject to the overall register at institution and group level. We recommend focusing subsidiaries considered to be material from a group perspective and risk-based approach.

Paragraph 47

Subparagraph a) point i: If we have correctly understood the example given in Annex 1, all sub-outsourcing arrangements of one provider should have same reference number as the original outsourcing. How are more levels of a sub-outsourcing chain to be shown?

Subparagraph a) point iv: Does each institution have to maintain an additional register, since all institutions in the EU already have to maintain a register to meet GDPR requirements? For local providers of local LEs out of the scope of the GDPR, there might be other data protection rules, which might mean that data is not comparable.

Subparagraph b): Extending the documentation requirements to all sub-service providers is unreasonable. That phrase should be deleted or limited at most to the sub-outsourcing of critical or important functions in line with section 10.1.

Subparagraph b) point vi: Please delete, as this information is already required to be maintained in GDPR registers.

Subparagraph c) point v): The EBA proposes that the outsourcing register should include the date of the last and the next scheduled audit, where applicable. We wish to point out that the dates of audits performed and planned are documented in the audit plan. To avoid redundancies, this information should not have to be documented twice (i.e. also in the outsourcing register). We therefore urge deleting paragraph 47c) point v). If not, please clarify whether the "next scheduled audit" means an internal audit or a risk assessment.

It should be clarified whether this date should consider external, internal or both audits.

Subparagraph c) points vi) and vii): Some outsourcing arrangements, especially within groups or financial networks (IPS), constitute a permanent division of responsibilities. The requirements for exit strategies therefore only have limited applicability in such cases (see also our comments on paragraph 89). For this reason, the phrase "where applicable" should be added to both points.

Subparagraph c) point ix: Please specify what is meant by the "specific nature of the data" (as it is the only data field not described in Annex 1).

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

Section 9/paragraph 48

Greater consideration should be given to materiality aspects in the advance assessments. We therefore recommend including an overarching reference to the principle of proportionality. The obligation to conduct due diligence in accordance with subparagraph b) should be expressly limited to the outsourcing of critical or important functions.

Section 9.1

The assessment criteria are highly detailed. The GBIC believes that the entire list does not have to be applied and documented to each outsourcing arrangement in order to classify a function as "critical or important" (or not). There are also overlaps with the actual risk assessment itself under section 9.3. We therefore recommend considerably streamlining section 9.1.

Paragraph 50 - editorial note: Articles 6 and 7 (rather than 7 and 8) of Commission Delegated Regulation (EU) 2016/778

Paragraph 50

Is our understanding correct that the outsourcing of mere (subordinate) parts of banking services (or operational tasks of internal control functions according to subparagraph b)) does not necessarily entail an assessment of whether they are critical or important? Otherwise almost any tasks (and parts thereof) performed by an institution would qualify as "critical or important".

Paragraph 51

Subparagraph a): Please rephrase: "*whether the proposed outsourcing arrangement ~~is directly connected~~ is direct part of the provision of banking or payment services for which they are authorized*"

Subparagraph c): Please delete as the contractual agreement's content is a consequence of this assessment (if it is critical or important, but (i) and (iii) do not apply, the outsourcing is not allowed – so this is not a criterion for assessing the criticality or importance).

Subparagraph e): Not feasible at consolidated group level: if there are several small outsourcings that are all non-critical or important for each group entity, the overall outcome should not be "critical or important". There might be a different level of "relevance" with overall counterparty risk at group level to be monitored, but not at the micro level for each and every outsourcing arrangement – this would run counter to the principle of proportionality.

Subparagraph h): It should be specified in Annex 1 whether "low" means "low substitutability" = "high dependency", as it could be confusing as currently defined.

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

The obligation to conduct due diligence on a service provider should be limited to the outsourcing of "critical or important functions". This is also necessary in light of the fact that such a classification is likely to happen in many cases because of the criteria given in section 9.1.

Please also specify to what extent such a due diligence check should be carried out.Paragraph 54

Our concern regarding due diligence requirements is that institutions are in some cases in a very weak position to negotiate with large service providers. Therefore, from our perspective regulators/authorities should support institutions by making service providers also comply with due diligence requirements.

A certification would help to respond in a better manner to the due diligence requirements set out in these guidelines. There would be a business case for them to serve all the EU banking industry, and each bank would not need to repeat the assessment. It could be easily provided by the market at a significantly lower cost and thus be more accessible for all players. It could include cybersecurity, data protection, physical security, business continuity and any other criteria supervisors deem appropriate. We believe that supervisors may still want to review the specific characteristics of a project, but much information would already be covered by the certifications, saving significant resources as the homologation processes are very costly.

Paragraph 56

Compared with paragraph 94 of the governance guidelines, the requirements constitute an unreasonable expansion and cannot actually be implemented in this extent. The GBIC therefore urges deleting this paragraph.

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

Paragraph 57

Please refer to our comments on paragraph 24. The text should be revised as follows:
"… relating to outsourcing arrangements ~~with third parties, regardless of whether or not those arrangement are considered outsourcing arrangement~~."

Paragraph 59

Subparagraph a) point i: Should be applicable only to external providers, as substitution of a group internal provider is a strategic option and not to be addressed at each outsourcing level.

Subparagraph a) point ii: The concentration should be covered at a consolidated level, and not at each single outsourcing contract level, as the person responsible for each individual outsourcing may not always be familiar with all the other contracts and services.

Subparagraph b): "…aggregate risks from outsourcing a large number of functions across the institution…" to be covered at the overall level, as they may not be known at each individual outsourcing contract level.

Subparagraph c): The requirement for significant institutions to assess step-in risk was presumably included in light of BCBS 423. However, the BCBS guidance does not contain any reference to outsourcing risk, and instead makes a distinction to operational risk (see paragraph 16). Subparagraph c) should be deleted.

Paragraph 61

Subparagraph d) points ii and iii: Conducting the relevant legal analysis on these matters would be particularly complex, expensive and burdensome.

Subparagraph d) point iii: If this were to be applied to non-critical or non-important functions, additional burdens would arise from analysing the laws of countries the bank is not domiciled in (or does not have a branch) for even minor contracts. The effort contradicts the business cases.

Subparagraph e): Please add “where relevant" as it should apply mainly to cloud services and ICT out-sourcings.

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?

Paragraph 62

We ask for clarification that a “written agreement” does not necessarily have to be present in hard copy but that also electronic formats are allowed as they have become common nowadays.

Paragraph 63

As mentioned above we understand that specific requirements of the guideline apply to critical/important outsourcings only. Otherwise, the requirements outlined in paragraph 63 for non-critical and non-important outsourcings would be too ambitious and not practice-oriented (e.g. agreement on comprehensive information, audit and access rights). We recommend focusing consistently on “critical or important” outsourcings.

Subparagraph b): Outsourcing arrangements can also be agreed for an indefinite term if termination rights and periods are defined. For the end date, the qualification “where applicable” should be added.

Subparagraph d): As this requirement is applicable to critical or important functions only, it should be moved to paragraph 64.

For the sake of completeness: this does not prohibit sub-outsourcing of non-critical or non-important functions.

Subparagraph d): As this requirement is applicable to critical or important functions only, it should be moved to paragraph 64.

Subparagraph g): The ability to require audit rights for all classes of outsourcing arrangements (critical or important or not) is too far-reaching. This should be requested only for critical or important contracts as these are the focus of the rules regarding internal audit in these guidelines.

Subparagraph h): The EBA proposes that there should be an unrestricted right to obtain any information needed with regard to the outsourcing and to access and audit the service provider, as further specified in section 10.3. An agreement for comprehensive audit and access rights should only be a minimum requirement when critical or important functions are outsourced. This requirement should be relocated to paragraph 64.

Paragraph 64

Is our understanding correct that the different elements should only apply/be included in the outsourcing agreement as far as these are applicable, relevant and proportionate in each individual case?

Subparagraph b: Precise quantitative and qualitative targets can be defined for each outsourced service. The phrase “where definable” should be added.

Subparagraph i): May conflict with local insolvency laws, as such clauses are not binding on the liquidator.

Subparagraph j): Please specify: (i) how and which powers are to be included and (ii) if national resolution authorities also include SSM?

Paragraphs 65–67

The guidelines outline detailed requirements for sub-outsourcing of “critical or important functions”. Do these requirements impact any kind of sub-outsourcing (complete chains) or just the first level of sub-outsourcing? It will not be possible to push all requirements to a third or fourth level of sub-outsourcing. Please provide a more practice-driven approach with regard to cloud computing and highly standardised cloud service providers with lean business models. It will just not be possible to agree these contractual requirements with a globally operating cloud service provider.

Paragraph 65a)

The EBA proposes that the outsourcing agreement should specify whether sub-outsourcing of any critical or important functions is permitted. If so, those activities that are excluded from sub-outsourcing are to be specified. We do not believe that this approach is practicable and suggest that the approval right of the outsourcing institution for sub-outsourcing, or concrete conditions for when sub-outsourcing of individual workflows and process steps is possible, should be anchored in the outsourcing agreement.

Paragraph 65d) and g)

There might be an inconsistency between Article 31(3) of MiFID II and paragraph 65 d). According to Article 31(3) of MiFID II, “The respective rights and obligations of the investment firms and of the service provider shall be clearly allocated and set out in a written agreement. […] The agreement shall ensure that outsourcing by the service provider only takes place with the consent, in writing, of the investment firm.”. However, the EBA guidelines only refer to “approval requirements” and do not specifically mention “consent”.

From our perspective, the outsourcing arrangement should indicate that when the service provider is allowed to sub-outsource and the customer has already given consent, there will be no need to ask for formal consent each time a subcontractor changes. Service providers will be only required to notify to the customer each time a new subcontractor is contracted.

It is doubtful in relation to these requirements if they can be implemented efficiently at service providers with a large number of clients. Moreover, such terms and conditions will be extremely difficult to enforce especially with large international groups. As described above, agreement on specific conditions for sub-outsourcing is sufficient as a minimum requirement. Subparagraphs d) and g) of paragraph 64 should therefore be deleted. Please also refer to our general comments.

Paragraph 65e)

In light of the need to reduce uncertainties associated with outsourcing, please define what you mean by “significant changes” to the subcontractors.

Paragraph 66b)

If paragraph 63 subparagraph g) is focused on critical or important functions, this should be the same here.

Paragraph 68

We would be grateful if the EBA could clarify if the meaning of “relevant providers” should be considered synonymous with providers supplying “critical or important” outsourcing.

Paragraph 70

The EBA should specify if this refers to a risk-based approach to locating data centres or to a country risk-based approach.

Paragraph 72

Paragraph 72 requires very extensive access, information and audit rights to be granted. The requirements should be limited to the outsourcing of critical or important functions in line with the principle of proportionality. As a minimum, there should be a differentiation or a sliding scale for other outsourcing arrangements; the same applies to the subsequent paragraphs in section 10.3.
The GBIC also wishes to draw attention to the fact that service providers must themselves take steps to meet legal requirements (for example data protection and information security). The unrestricted granting of rights to the outsourcing institutions is therefore unlikely to be permissible and enforceable. Please reword these paragraphs appropriately.

Paragraph 74

The EBA proposes that, without prejudice to their final responsibility for the audits, the institutions/payment institutions may use third-party certifications and reports made available by the service provider. However, they shall not rely solely on them.

This means that the internal audit function must conduct additional audits of the service provider, regardless of the quality and quantity of the available third-party certifications and reports. We suggest that, irrespective of the access and audit rights, the internal audit function may decide whether the information made available by third-party certifications and reports is sufficient, or should be supported by its own audits. In the case of corresponding (full coverage of the outsourced service) and adequate (controls and audits) certification by a qualified certifying or auditing party, it should be possible for internal audit to dispense with its own audits (see also the original EBA/REC/2017/03, 28 March 2018, Recommendations on Cloud Outsourcing, section 4.3, 8)(b)). Otherwise, it would not be possible to work together with major service providers such as Microsoft Azure or Amazon Web Services (AWS). We therefore urge amending paragraph 74 as follows:

“*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~~ scrutinise the reliability, relevance and sufficiency of the information provided and decide whether further action is needed.*”

The EBA should clarify that the audit function of the service provider itself can also perform the audit in the case of a service provider with a banking license and hence its own audit function according to banking standards.

Paragraph 75

In addition to pooled audits, audit reports by the service provider's internal audit must also be considered to be equivalent; see paragraphs 46 and 47 above.

Paragraph 76

Section 10.2 contains adequate detailed requirements for ensuring information security. It is a big step to require institutions to expect service providers to grant them rights to conduct security stress tests at the service providers, based on a control requirement in the EBA guidelines on ICT Risk Assessment. Such tests may often entail liability risks and should therefore always be commissioned by the service providers themselves.

To ensure effective cybersecurity protection, there should also be no unilateral focus on penetration tests as an approach, but rather the use of various prevention, detection and reaction measures that are appropriate to the situation and the risks.

We therefore suggest deleting paragraph 76.

Paragraph 79

In paragraph 79, "alternative ways to provide a similar level of assurance" are cited but not specified at all. Especially the required penetration testing from paragraph 76 would create a risk for another client's environment in the case of a public cloud. We would urge the EBA to provide more explanations in respect of alternative solutions.

Paragraph 81

Is our understanding correct that it is sufficient if local law provides for such termination rights even if not expressly mentioned in the contract?

Subparagraph c) (1.) this should be only applicable to critical or important functions. (2.) "(such as sub-outsourcings or changes of subcontractors)": delete "subcontractors" as not subject to rules in 10.1 and contractually agreed approval mechanism according to paragraph 63d).

Paragraph 65e)

The current wording is ambiguous and could give the supervisory authorities inadmissible scope for instructing institutions to terminate outsourcing arrangements. For example, a national competent authority could decide that it is difficult to supervise outsourcing arrangements with foreign service providers (including locations in other EU member states), which would be questionable, including under competition constraints aspects.

Paragraph 82

Is our understanding correct that this applies only to critical or important functions due to proportionality aspects? Please add "for critical or important functions or where otherwise appropriate".

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

General comment: The required monitoring of security requirements according to paragraph 69 in section 10.2 is also part of the oversight.

Paragraph 87

Subparagraph b): “Key control indicators” (KCI) are intended to cover the overall set-up of a control system (different from KPIs or KRIs covering respective services or risks). We deem it not appropriate to apply KCIs to each contract.

Subparagraph c): Should be applicable only for functions that are critical or important or otherwise critical in process continuity.

Paragraph 88

The term “indication” is not further defined in this paragraph. This could therefore refer to any kind of observation being made by either the institution/payment institution or the service provider that service providers may not be carrying out the outsourced critical or important function effectively, or in compliance with applicable laws and regulatory requirements, as soon as the institution/payment institution becomes aware of this. In addition to that, the differentiation between “indications” and “recommendation/findings” (as mentioned in section 7, paragraph 48) is not clear. We question if all follow-up activities should be performed by the internal audit activity of the institution/payment institution or if resolution of corrective actions regarding “indications” should rather be followed up by the institution's provider management/retained organisation, and only audit recommendations/findings are followed up by the internal audit function.

It is our understanding that only audit recommendations/findings of the audit activities of the internal audit function of the institution/payment institution (please refer to section 7, paragraph 45) are followed up in detail by it, and the follow-up of resolution of corrective actions regarding “indications” is performed by the institution's provider management/retained organisation.

Please clarify that the follow-up activities by internal audit relate solely to its own audit recommendations, whereas following up corrective measures would be the responsibility of the relevant division of the institution.

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

Paragraph 89

Some outsourcing relationships in the financial sector, especially in consolidated groups or among entities of a financial network related to an IPS, are characterised by a permanent division of functions and specialisations. In Germany, for example, the savings banks and cooperative banks have outsourced much of their IT to the centralised data centre of the respective financial network. Because of the ownership and governance structures within the groups and networks (IPS), the likelihood that a service provider will be terminated or will fail is extremely low. If the quality of service would deteriorate, the client institutions have adequate opportunities to intervene.
Developing clearly defined exit strategies for such outsourcing arrangements would require an unreasonably high and also unnecessary effort. The GBIC is calling for the addition of an exemption for intra group

outsourcing and outsourcing in an IPS, including entities that are members of the network. The same goes for outsourcing to centralised service providers.

Paragraph 90

An exit plan cannot literally be tested. The word “tested” in subparagraph a) should be replaced by “scrutinised”. The words “and sufficiently tested” in subparagraph b) should be deleted.
Please also clarify in subparagraph a) that the safeguards for terminating an outsourcing agreement should not include obtaining concrete quotations from alternative service providers. This would also lead to considerable effort on the part of the service providers themselves. In addition, some services are only offered by dominant providers (monopolists), with the result that it is not always possible to obtain competitive quotations.

Paragraph 91d)

Regarding “success criteria for the transition”: What should they look like? Normally the process should run at a defined service level in a new contract, (maybe with initially reduced service level, a grace period, as included in many new contracts).

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.

Paragraphs 92 to 95

The information duties spelled out in these paragraphs are very burdensome and have the potential to significantly delay planned outsourcing transactions. In particular, it may be unclear whether the planned transaction can be implemented as long as the competent authority has not yet advised on its assessment of the planned transaction. The information which EBA expects to be notified is quite complex and would normally be available only in final format after negotiations have been finalised. Similar to the case of M&A transactions, once such negotiations are terminated, all parties are under pressure to implement the arrangement very soon, in particular because key staff may tend to leave the enterprise due to uncertainties arising in connection with the changes. A further waiting period arising from discussions with the competent authority may last several months. In our view, communication with the competent authorities should be left to existing national practice and/or regulation. In Germany, for example, the annual auditor must report on the relevant new material outsourcing transactions made during the audited business year. The supervisory authorities obtain a concentrated overview on this basis. Of course this happens ex post, but as a compensatory measure, the competent authorities should have the right to request unwinding (or amendments of) any outsourcing arrangement that would not comply with the national rules set up under the guidelines.

Paragraph 92

We consider the requirement to make available the register of outsourcing arrangements to the competent authorities in a “common data base format” as critical. The institutions currently use custom database solutions for their outsourcing arrangements. Populating and subsequently maintaining a database format that might be stipulated by the competent authorities would entail a considerable (initial) effort

for the institutions. We therefore suggest removing the requirement to make the register available in a common database format. If this is not decided, please clarify whether a common database format is supposed to be used, or whether the format of the report in which the data is made available is meant.

A common data format would probably be based on the very extensive information requirements of the ECB for the SI SREP and thus violate the principle of proportionality. The arrangements for collecting information for the SREP should therefore be a matter for the competent authorities.
In the GBIC's opinion, the register to be made available to the competent authorities should not be understood to mean all of the internal documentation to be maintained internally by the institutions in accordance with section 8 and Annex I. The GBIC is calling for this to be explicitly clarified. Providing basic information such as the brief description of the outsourced function, whether it is considered critical or important, and the name and the registered address of the service provider is sufficient (paragraphs 47a)i), ii) and iii); b)i) and ii). If they need to, the competent authorities can obtain a more detailed insight at any time in an on-site inspection or through ad hoc inquiries.

Paragraphs 93 and 94

The proposed information requirements for the institutions will not generate any justifiable value added. The requirement for advance notification from CEBS GL02 was also not implemented by many competent authorities in the past for good reasons.
The advance notifications would cause considerable additional effort at the institutions. In light of the opportunity for competent authorities to intervene – although this is only mentioned in the accompanying documents to the Draft guidelines – there is also legal uncertainty for the institutions about when the contract with a service provider can be effectively entered into (operational risk may also arise because of delays). At the same time, the flood of information at the supervisors mean that they can hardly be expected to actually make use of the opportunity to intervene. This applies in particular to LSI supervision.
Last but not least, the institution is responsible in the first place for the admissibility of an outsourcing arrangement. Any supervisory intervention rights would curtail the management powers and responsibility of the governing body.
In general, the provision of the regular overview by the institutions in accordance with paragraph 92 should be sufficient. For the reasons shown above, the GBIC is calling for the requirements in paragraphs 93 and 94 to be deleted without replacement.

Paragraph 95

In line with the arguments advanced regarding paragraphs 93 and 94, the GBIC urges deleting the words "material changes and".

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

Paragraph 103

Any reputational risks arise from operational risks. We regard a separate examination and assessment by the competent authority as unnecessary and urge the deletion of subparagraph b).
With regard to subparagraph c), please see our comments on paragraph 59c). The point should be deleted.
Additionally, there is no justification for the general presumption of conflicts of interest, as assumed in subparagraph g). As a minimum the words "where relevant" should be added.

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

In line with footnote 23 on paragraph 47, it should be clarified that the Excel template is merely one way to present the documentation, and its use is voluntary.

- Data field “specific nature of the data not held”: we do not understand the meaning. Please specify the meaning or purpose of this field.
- The data field “substitutability” might be confusing in terms of the definition. A definition as used by the EBA (“Easy”, “Difficult” or “Impossible”) would lead to broad scope for interpretation and presumably confusion. We recommend providing more guidance, e.g. in terms of “time needed to shift” or “resources that are necessary”, etc.
- How should sub-outsourcing chains be marked? How to multiply group providers that are sub-outsourcing to several other providers without multiplying capture of the same data?

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.)?

As explained under “General comments”, the GBIC believes that the Draft guidelines and the obligations proposed for the institutions go far too far overall. There is no reasonable balance between cost and benefit. There is a risk that institutions will no longer be able to exploit the opportunities offered by outsourcing because of legal uncertainties and the high administrative effort, as well as the ongoing controls.