Consultation response

EBA Draft Guidelines on Outsourcing Arrangements

24 September 2018

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to respond to the EBA's consultation paper on its **Draft Guidelines on Outsourcing Arrangements (referred to hereafter as "the Guidelines" or "GLs").**

Our response starts with our overarching comments on the proposed GLs, which highlight our main concerns, and is followed with more detailed responses to the individual questions posed in the consultation.

I. Overarching comments

Definitions, scope and timing of implementation

AFME is concerned that the proposed definition of outsourcing will lead to many arrangements that are not typically considered to be outsourcing arrangements becoming subject to the requirements in the proposed GLs. Combined with the approach to what is then critical or important means that registers, risk assessments, policies, audits, concentration limits and other requirements will attach to an ever longer list of activities. The question of how far to look through sub-outsourcing arrangements further amplifies the associated compliance burden. At present it is unclear how the GLs sit alongside the proportionality principle or how relevant and manageable they will be for institutions and Competent Authorities (CAs) in practice.

Our response to the consultation questions below provides suggestions on how to better streamline these definitions as this will be key to avoid creating substantial and unnecessary compliance and monitoring burdens which might otherwise divert supervisory attention from those arrangements that could materially impact the risk profile of an institution.

We understand the EBA's approach to integrating its cloud recommendations into these more general GLs. However, we think that several of the difficulties in these GLs reflect the complications of trying to address cloud computing and more general outsourcing, including so-called empty shell concerns, within a single document. Many of the problems of definition, scope, and proportionality pointed out in our response below could be helped by the recognising the unique complications, but also opportunities, presented by cloud computing within financial services.

Unless the final GLs achieve a clearer and more restricted approach to their scope, as proposed, the timing of implementation (before 30 June 2019) is unlikely to be achievable.

Finding the appropriate balance between managing and monitoring risk and business efficiency

The GLs as currently drafted give CAs the possibility to limit or restrict the scope of outsourced functions or to require an exit from the arrangements. However, the Guidelines do not give any qualifications for what would lead to an CA taking action on this scale. This, as well as the proposed notification requirements, if not consistently applied or understood clearly as to their purpose, ultimately creates substantial business case risk for firms which could limit or handicap the use of outsourcing by regulated firms.

Combined with the substantial compliance burden noted above, we find it difficult to reconcile the overall approach of the GLs with other key supervisory priorities regarding bank business models and profitability. We strongly encourage the supervisory community to reflect on this further when finalising the GLs.

We also wish to draw to the EBA's attention many of the requirements in the draft GLs will present issues where banks themselves act as an outsourcing provider to other banks. To avoid unnecessary duplications when outsourcing is provided by an institution subject to an equivalent or the same outsourcing regime, these arrangements should be excluded from the requirements.

Better linking common supervisory objectives by recognising existing work and other areas of regulation and in particular recovery and resolution planning

We recognise the need for, and support the application of, the GLs to intragroup outsourcing arrangements. We note that this is in line with existing regulation and risk management. We are concerned however that the GLs do not adequately reflect the difference in risk profile between intragroup outsourcing and outsourcing to third parties. Without acknowledging the cases where there are legitimate benefits associated with intragroup arrangements, there is a risk of creating undue burdens for firms with such arrangements, without any material improvement in risk mitigation.

Driving this concern is the lack of recognition in the GLs of approved global recovery and resolution plans and the various structures and approaches firms have set up and taken to be increasingly resolvable. It is essential that these aspects be integrated into the supervisory assessment of compliance with the GLs and that firms are not required to unnecessarily duplicate, or unintentionally contradict, the work that has gone into putting these plans into place. As recognised by the EBA itself in its latest SREP Guidelines, it is necessary for both supervised institutions and competent authorities to leverage the complementarities and synergies between SREP and recovery plans. We would like to see this occur more in practice and are at the EBA's disposal to consider how this can be done further.

Cross-border groups may experience particular burdens implementing these GLs

The cumulative burden of the requirements for KPI monitoring implied by the proposed definition, together with the proposed approach to intragroup outsourcing and the need to manage multiple, differing regulatory approaches to outsourcing across the globe is likely to particularly penalise international banking groups with multiple subsidiaries outside of the EU or those that may centralise services within their home jurisdiction when it is located outside the EU.

We encourage the EBA to elevate the need for coordination amongst the international supervisory community, particularly with respect to standardisation of data collection and use of the information contained in the proposed register.

Outsourcing to cloud service providers – an ongoing issue requiring further reflection to avoid limiting technological progress and costs efficiencies important for the financial services sector in line with supervisory priorities

The question of industry-wide concentration risk to CSPs, three of which dominate the global market, should be addressed by the broader regulatory community in greater detail and with some urgency. We appreciate the efforts the EBA is already making in this area and encourage it to continue to foster dialogue between the industry, providers and the relevant authorities to find pragmatic solutions to address the underlying issues and risks. AFME is of course willing to contribute to this ongoing work.

No single firm can monitor the concentration risk of the industry to any one or all of the CSPs. We understand that one of the purposes of the register of outsourcings required by these GLs is to give regulators the ability to monitor the aggregate industry exposure. The industry accepts this rationale to the extent that the information required is necessary for this purpose. However, without ultimately establishing their own risk appetites on the basis of clear taxonomies (which we recognise will take time to define), regulators are likely to interpret the information collected via these GLs in different ways which could result in firms encountering divergent regulatory approaches. For instance, one CA may determine that a firm's outsourcing to a specific provider results in an inappropriate concentration of the industry and, as a, result, block or require exit from the arrangement. Simultaneously a different CA could take a different approach by allowing more material outsourcings from a different firm to the same CSP. Thus, coordination among relevant CAs is essential. We therefore recommend that the EBA coordinate CAs to establish risk appetites in consultation with the industry. This question is likely to be of global concern and thus early consideration by EU regulators will be helpful.

Moreover, as the use of cloud computing by the industry expands and the systemic importance of the CSPs increases correspondingly, we also think it is important for the broader regulatory community to consider requiring the creation of living wills for data centres in order to ensure continuity in the event of e.g. the supplier's insolvency, a systems failure or catastrophic event. Although particularly relevant in financial services, this issue is likely to grow in importance for other critically important sectors. Regulators from across the critically important sectors should work together to consider the merits of this risk-mitigation measure.

We recognise that one of the concerns related to concentration risk is the contraction in the overall number of data centres out of which global financial services are run. Market demand and continuing geographic diversification should help to combat this concern. However, until such time as regulators feel the market is sufficiently diversified that this is no longer a substantial concern, the solution of requiring living wills for CSP data centres should be considered as a reasonable precaution not only for the financial system, but for the resilience of the broader economy.

AFME believes there is a need for continued discussion of how to address the potential systemic importance of service providers who dominate the market. The industry is of the view that, in order to ensure stability, financial regulators will eventually need to rely on more than the contractual relationship between those providers and regulated firms. This may for instance

include directing monitoring of the providers, but further debate and engagement on precisely what form this should take is needed urgently and at senior level.

Finally, we appreciate that one of the reasons for these GLs is to assist the industry in clearly setting out to its suppliers what needs to be in place the purposes of ensure stability of the financial system. We would very much welcome further assistance from the EBA to help reach these goals. For instance, inclusion in the final GLs of clear, schematic representations of which sections of the GLs apply in which cases would help the industry engage with its providers. Beyond the present GLs, any efforts by the EBA to promote financial service sector certifications, in line with the works of the European Commission Working Group on *Cloud security certification scheme*, where it is able to do so would be extremely helpful. This would tremendously help increase the efficiency (and overcome some of the cost/benefit issues discussed above) by reducing the need to have each bank in the system repeat assessments of the same providers.

II. Responses to the consultation questions

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?

Scope

As proposed, the definition of outsourcing, including the approaches to sub-outsourcing and "critical or important" outsourcing arrangements, are too broad and could bring into scope almost all types of contractual arrangements, bar a few specified exceptions. Our members *do not* consider many of these arrangements to be outsourcing and have significant concerns that the proposed approach would place an extremely heavy compliance burden on the firms subject to these GLs.

We consider that, instead of aligning with the MIFID II approach, the definitions in the GLs go beyond what is set out in the associated Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II as

i) TheMiFID requirements only apply to the outsourcing of "critical or important" functions and not to all outsourcing arrangements as proposed by the EBA in the present GLs
ii) Art 30.2 of the Delegated Regulation clearly limits the scope of those functions that should be considered to be "critical or important" by specifying that the provision of advisory services (including legal advice or personal training) or the purchase of standardised services including market information services and the provision of price feeds should be excluded from this definition
iii) The proposed guidelines for assessing the criticality or importance of outsourcing arrangements (set out in para 50 of the consultation) can be read to mean that all activities and process linked to core business lines could be classified as critical or important arrangements.

To better target their scope, we recommend that **para 23** of the GLs be redrafted to include the functions specifically mentioned in Art 30.2 of (EU) 2017/565 and specify that this list of examples is by no means exhaustive. We also suggest changing the wording in para 50 so that the critical and important notion is clearly understood as being limited to those that are directly connected to the provision of core business lines and critical functions (see our comments on para 50 further below). Moreover, in comparison to outsourcing definitions commonly used by the industry, we also find that the concept of an *ongoing relationship* with the provider is missing from the EBA's approach. We would therefore also welcome recognition of this feature of arrangements in the final definition. Finally, it should be clear that the use of cloud technologies should not be necessarily considered per se a case of outsourcing. This consideration should depend on an analysis of the activity and processes and not the technology used. The mere fact of using cloud technologies should not trigger the consideration of outsourcing.

Additionally, we think there is an important contradiction in the definition of outsourcing given in para 11 (outsourcing is an arrangement that would otherwise be undertaken by the institution itself) and para 22 in the section describing outsourcing arrangements which states that "when conducing 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 would be able to perform it by itself." This latter definition would bring into scope a significant number of processes that we do not believe the EBA intend, for instance the calling of a cab or Uber could be considered outsourcing under such a definition. It may also extend to market connectivity.

To the extent they have not already done so, we also encourage the EBA to consider the approaches adopted by other jurisdictions in this area. As an example, the Monetary Authority of Singapore has created a cloud specific annex to its outsourcing guidelines and has defined outsourcing in a manner that is closer to how the industry views the concept.

Beyond the outsourcing definition itself, as proposed, the definition of, and approach to, sub-outsourcing is not operational. The final GLs will need to take a more practicable approach to sub-outsourcing, balancing the need for firms to look through to the relevant risks potentially posed by subcontractors in their material outsourcing arrangements with the overarching principle of proportionality. We suggest that the key considerations in this respect involve assessing whether the outsourcing is related to a critical or material function (as set out in the MiFID II approach) and then the reliability of the outsourcing service provider. Our assumption is that all regulated activities are critical or important. On non-regulated activities, the consideration of whether a defect or failure in an activity may impair a firm's operations should be approached by the institutions themselves, looking at the relevant risks with the overarching principle of proportionality.

We think that the only way this can be achieved in practice is by explicitly limiting the scope of the relevant requirements to sub-outsourcing of critical or important functions and only for those services directly linked to the delivery of such outsourcings (please also refer to our comments on para 60 below).

We also note that the definition of sub-outsourcing on page 11 refers to the "further transfer" of a process, service, activity, etc. To avoid any misunderstandings or unintentional extension of the scope of the sub-outsourcing concept in relation to outsourcing itself, this should be changed to be consistent with the use of the term "performing" activities, services, etc. used in the outsourcing definition.

Finally, to facilitate their reading and firms' compliance, we would welcome the inclusion of a diagram in the final GLs specifying which sections of the requirements apply to or are relevant for general outsourcing arrangements, outsourcing of a critical or important function, intragroup arrangements, outsourcing to third countries, outsourcing of authorised activities and any other categories should they be introduced.

Implementation

As proposed, the timing of implementation (before 30 June 2019) is unlikely to be achievable given the scope issues noted above.

We welcome the EBA's recognition of the fact that firms will need more time to build up their registers for existing arrangements through the granting of the transitional provision. However, we think that both the implementation deadline and transitional arrangements should both be postponed by at least 12 months in order to make the workload manageable for firms. We also recommend that the build-up of the register occurs in two phases – one for critical and important functions, with other arrangements to follow.

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

Paras 17 and 18: We appreciate that the EBA has set out these Guidelines consistently with the level of application of the CRD/R and note that compliance should have regard to the principle of proportionality. Should there be changes to level of application via the level 1 text, we would of course welcome an update of the Guidelines accordingly. In this context, we recall the ongoing level 1 discussions on the new prudential regime for investment firms. Should so-called class 2 and class 3 investment firms be removed from the scope of the CRD/R, the GLs should take this into account.

Nevertheless, we think it is still necessary to clarify in the final GLs what the expectations are (e.g. in terms of notification requirements) should outsourcing occur between subsidiaries of EU groups located in third countries. We also note that subsidiaries in third countries may be obliged to follow requirements that could potentially be either in addition to[1] or in contradiction with certain areas of these GLs. It is important that competent authorities take this into account when monitoring compliance of the GLs, particularly given their non-binding nature.

[1] The Monetary Authority of Singapore and the Hong Kong Monetary Authority, for instance, also require the submission of a register from regulated firms. For firms operating globally the effort of complying with growing requirements for information on outsourcing is becoming a major demand of resource. In addition, the inconsistency of definitions and requirements of such registers means that different authorities may take contrasting or even contradictory views of the current risks and required action which could lead to substantial disruption across the industry.

Approach taken throughout the GLs with respect to intragroup outsourcing

There appears to be an underlying assumption in the GLs that intragroup outsourcing could be inherently more risky than other (i.e. third-party) outsourcings. For example:

- in paragraph 20 (a) the proposed requirement for "independent" monitoring of the service provider, on which we would welcome clarity both on what is intended and on the rationale with respect to intragroup arrangements;
- reference in paragraph 38 to conflicts of interest between entities within the same group;
- references in paragraphs 51 (e) and 59 (b) on aggregated exposure to the same service provider;
- reference in paragraph 59 (a) on concentration risk.

Additionally, the background section of the consultation paper singles out service providers located outside the EU as creating specific risks and urges a "strict framework" for outsourcing to third country entities, which is likely to impact in particular firms headquartered or with significant operations outside the EU.

Global banks are generally organised as integrated structures and often rely on significant centralised intragroup service provision to ensure that they can be run on an efficient and profitable basis. Such a model ensures that both the service provider and the recipient operate within a common risk framework under common management, ownership and branding, leading to an alignment of incentives. Influence over decision-making, access and data protection processes, for example, can deliver a more streamlined, transparent, controlled and consistent approach (than outsourcing to a third-party). Moreover, intragroup outsourcings are usually to the same entities, which have a known track record whereas using third parties can often involve an entirely new relationship with an unknown entity. Finally, intragroup outsourcing can be more flexible and easier to conclude.

The GLs should not lead to the unwinding of intragroup arrangements particularly where this could then create heightened risk in other areas (such as those mentioned directly above), which could lead to unintended impacts on operational resiliency. While the CEBS 2006 Outsourcing Guidelines mentioned concentration risk (at a sectoral level – guideline 12), they also acknowledged that the ability of the service recipient to influence the service provider in the group context is helpful and relevant to weighing up the overall risk of such arrangements.

Intra-group outsourcing should also be recognised in the context of global recovery and resolution plans and shared servicing agreements rather than applying replacement tests for third-party outsourcers. At present the GLs come across as being developed in a silo from the existing requirements for firms' recovery plans and for instance the requirements related to the content of such plans as set out in Section A of the Annex to the BRRD and the final RTS on the content of content of these plans[2].

While clearly not the only approach that can be adopted to comply with the requirements of the BRRD or similar international frameworks, as an example, some firms have set up bankruptcy-remote service companies to supply common group services such as IT, HR, certain risk management and financial reporting services, etc. These "servcos" are aimed at increasing resolvability and ensuring the continuity of critical functions. They form part of a group's RRP, as approved by their home resolution authorities, which will already have taken into account many of the risks identified, such as exit strategy.

[2] See for instance Article 7 of this RTS

As a further specific example, many firms run their own IT servco, serving entities across the group. As part of the same group, and as a result of working with a single IT servco, there is stronger goal congruence enforced by governance resulting in lower risk overall. From the GLs as currently drafted one might deduce that a firm is unduly exposed to its own IT servco and react by decentralising some IT services. This approach would lead to less consistency and harmonisation of IT across the group with corresponding implications for IT resilience and the services this supports.

As currently drafted, the GLs do not recognise these approved recovery and resolution plans and the structures firms have set up to be increasingly resolvable. It is essential that the they be integrated into the supervisory assessment of compliance with the GLs and that firms are not required to unnecessarily duplicate (or unintentionally contradict) the work that has gone into putting these plans into place. For firms with activities in multiple jurisdictions, supervisory cooperation in order to ensure that the relevant information is being shared and taken into account with respect to outsourcing arrangements is paramount.

AFME also thinks it is important to consider the interlinkages between the proposed guidelines and the work done *on operational continuity* in recovery and resolution planning. For example, the FSB guidance on arrangements to support operational continuity in resolution acknowledges that different approaches may be appropriate for different service models. These have been applied by some resolution authorities as part of their resolution planning and some firms have already put in place robust structures to address these concerns. We understand the SRB is also currently considering its approach. As national competent authorities apply the GLs, they should coordinate with the relevant resolution authorities to avoid duplicative or contradictory requirements.

We encourage the EBA to ensure that its member supervisory authorities are coordinating within their own internal structures so that the information provided in the context of recovery plans is shared (inter alia) with the relevant teams in charge of monitoring compliance with the present GLs, which form part of the EBA's "suite of SREP-related guidance". As clearly stated in the updated SREP Guidelines[3], "Competent authorities should reflect in the SREP assessments available information and outcomes from all other supervisory activities, including […] assessment of recovery plans […]. Feedback received from our members indicates that the complementarities and synergies identified between SREP and recovery plans in the SREP Guidelines are not being sufficiently leveraged in practice.

Similar cooperation and information sharing should also take place between supervisory and resolution authorities. Moreover, various means such as supervisory colleges should be used to ensure that the relevant information contained in group recovery plans is provided to EU competent authorities by the relevant home authority for third country groups. We invite the EBA to investigate any obstacles to data sharing that may arise in practice (e.g. potential absence of MoUs) so that these can be addressed. We believe that the features of intragroup services provision discussed above mean that outsourcing to a limited set of group service providers can be very beneficial so long as implemented in a controlled and systematic way. When this is the case, intragroup outsourcing will in general result in lower risk to a group overall than outsourcing to third parties. We therefore consider that the quality of a firm's intragroup risk management, measurement and controls and internal governance in general should be factors explicitly recognised in the final GLs. Practically speaking, this should be integrated into the

[3] EBA SREP Guidelines of 19 July 2018 – see in particular pages 14-15

respective requirements for intragroup arrangements in these GLs to provide a more balanced and proportionate assessment of the overall risks of intergroup outsourcing arrangement.

Particular areas of the GLs where greater recognition of the approaches set out in recovery plans, the benefits of intragroup arrangements when conducted in a controlled manner and/or the linkages between these various aspects include:

- Section 5 on conflicts of interest
- The criteria for assessing criticality or importance in para 51 (which currently appears to be drafted solely from the point of view of a third-party arrangement)
- The sections of the draft GLs relating to due diligence (section 9.2) and risk assessment (section 9.3)
- Requirements related exit strategies (section 12) should reflect group recovery and resolution plans.

Finally, we note that benefits accrue irrespective of the location of the shared service providers (in or outside the EU) so a third country provider should not necessarily be assumed to be riskier or to require the imposition of additional hurdles.

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?

Outsourcing vs purchases

Para 23 As mentioned above, this list of examples in para 23 is too narrow and, as currently drafted, coveys the impression that the intention of the GLs may be to treat many contracts that the industry considers to be purchases as outsourcings. While we appreciate the difficulties associated with providing lists of examples within the GLs, there is nevertheless a need for a clearer distinction to be made between purchases and outsourcings, while also considering potential future technological developments. Cases where institutions are purchasing third-party services akin to utilities should be excluded from the scope of outsourcing [4], The final GLs should at least clearly specify that any examples provided are not exhaustive.

[4] For example, cloud arrangements where the data centre and cloud infrastructure is owned by the bank, but where the bank uses third-party software to access the cloud should be out of scope and not considered outsourcing but purchases of a third-party service. Similarly, situations such as those that occur in "Infrastructure as a Service" (IaaS) contexts where the institution is only "outsourcing" the underlying infrastructure but retains internally the relevant business activity or process for which that underlying infrastructure is required should not be treated as outsourcings. IaaS is more aligned to "buying-in" the supply of a commodity or tool, rather than the outsourcing of an activity or process.

Application to *all* arrangements with third parties

Para 24: We understand it is not the EBA's intention to apply these GLs to all third-party arrangements. We also recognise that third-party arrangements must be addressed by firms' risk management, and in particular their operational risk management.

As operational risk management is broader than the outsourcing GLs, it is not clear why it is necessary to specify that the due diligence requirements set out in paras 53 and 55 and the risk assessment requirements of Section 9.3 of these GLs apply to all arrangements with third parties, even if these arrangements are not qualified as outsourcing arrangements.

Our members find this wording to be contradictory to the proportionality principle and view it as potentially amounting to a substantial extension of the scope of the GLs that could dramatically increase the compliance burden for firms when these legitimate concerns of supervisors are already addressed elsewhere.

We consider it would be preferable for the EBA to recall or cross-reference to existing operational risk managements requirements for firms rather than introducing these paragraphs which could give rise to significant misinterpretations.

Outsourcing to third countries of activities requiring an authorisation or registration in a Member State

Para 26: we are concerned with the need for formal cooperation agreements to be in place with third countries given that outsourcing is likely to be in place with entities in countries where such agreements are not yet in place and where there is uncertainty with respect to the timing of their finalisation.

While we fully agree on the importance of supervisory cooperation, and recognise that this requirement relates only to the full outsourcing of authorised services[5], we note that in the impact assessment presented in the GLs, the EBA considered the possibility of adopting an outcomes-based approach that would allow the promotion of effective supervision through a variety of other mechanisms rather than an approach that would require the negotiation and finalisation of an MoU in every case before such outsourcing can take place, particularly in third countries with well-developed regulatory frameworks (US, UK, Japan etc.).

This could become a concern and significant business constraint if capacity or political constraints were to lead to supervisory cooperation agreements suffering from undetermined delays.

Consequently, AFME would prefer Option B under D. 7 (pp56-57 of the impact assessment) – i.e. institutions must be satisfied that their home competent authority can effectively supervise them - and the competent authority would have the power to step in if this were not the case – to be the default option until relevant cooperation agreements are in place. Otherwise institutions may be prevented from carrying out and entering outsourcing arrangements for an unforeseen amount of time until singed MoU agreements are put in place with significant numbers of third country authorities globally.

[5] As clarified in the EBA's public hearing on these GLs

We note further that when the relevant competent authority responsible for monitoring compliance of these GLs will be part of an international supervisory college the need for formal MoU agreements to be in place to ensure that the relevant information is shared between the relevant authorities involved in supervising a group should also be less acute.

Moreover, we understand that para 26 applies specifically to the *complete* outsourcing of an authorised banking activity or payment services. Consequently, when the outsourcing arrangement relates to a service or process underlying such an activity, a formal MoU would not need to be in place. To avoid misinterpretation going forward, we suggest that this be explicitly mentioned in the final GLs (while recognising that the appropriate access rights etc., as with other outsourcings, would still need to be in place), with language clarifying exactly what this concept intends to cover. Para 26, but also para 49 and Title V should be adapted accordingly.

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

The level of compliance burden associated with this section is linked to the questions of definitions, scope and level of application of these GLs which require clarification as already noted. It is also essential that the proportionality principle be more clearly embedded into this section of the GLs.

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

Conflicts of interest

In order to avoid confusion and ensure alignment with Section 5, the pre-outsourcing analysis requirement in Section 9 to "identify and assess conflicts of interest that the outsourcing may cause" (paragraph 48.d) should be rephrased as "identify and assess **material** conflicts of interest that the outsourcing may cause"

It is also unclear what the EBA is concerned about with respect to such issues occurring in an intragroup context if the relevant governance is in place and arrangements are conducted at arms' length.

The provision of examples would therefore be helpful to clarify the underlying concerns in this section.

Internal audit function

We take the view that internal audit should not substitute for first or second line responsibilities and that internal audit's role is one of overview of the process and controls rather than the actual direct supervisor of the outsourcing arrangements. The EBA's approach under the draft guidelines in Section 7 would involve a blurring of these lines, resulting in a step away of the role on an internal audit function.

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

While we fully appreciate the need to document outsourcing arrangements appropriately, as proposed, we find the content of the register to be too detailed, in certain instances referring to terms that are not defined in a manner that will enable the collection of homogenous information, and with information requirements that will potentially need updating at a frequency that is likely to be beyond what is useful from a supervisory point of view.

We also think more background on the way in which supervisors will use this information is necessary. The EBA should require CAs to detail what decisions they will make with the register, how it will be used, what policies it will affect and how they will set their own risk appetite e.g. for concentration risk in certain sectors (see above in our overarching comments section).

We recognise that one of the register's uses is to progressively build up a picture of concentration risk to outsourcing providers across the sector, something that indeed needs to be done by supervisory authorities rather than individual institutions. However, it is not clear whether the register will be sufficient to fulfil that purpose as there are likely to be differences in interpretation from both institutions and CAs with respect for instance to the proposed classifications of cloud outsourcing (see question 15 for more information).There is also a need to clarify whether the template presented in the annex is intended to be the "common database format" referred to in the draft GLs. Finally, we recommend the wording in para 47 [the following information] "should at least be included" needs to be changed as otherwise different CAs will adopt different approaches which would not be consistent with efforts to foster the standardisation necessary to build aggregate pictures, could substantially increase the compliance burden for firms in certain jurisdictions and ultimately goes against the level playing field approach the GLs are trying to foster.

- **Para 47a:** we note that point iii) does not feature in the excel template and that point v) requires clarification in the context of sub-outsourcing
- **Para 47b:** institutions are unlikely be able to comply fully with these documentation requirements in practice particularly at the level of sub-providers in the manner currently suggested by the draft GLs (as this information is not disclosed to them, in particular by cloud service providers). As mentioned in our response to question 3 above, we think that in practice, the best way to address this issue and achieve the appropriate balance is for 47b to be applicable to sub-providers only in cases of outsourcing critical or important functions. It must also be clear that the proportionality principle applies in such cases too. In line with the view expressed in our response to the section on sub-outsourcing below, the content of the register should be adapted if alternative solutions such as information regarding the main service provider's sub-outsourcing policy is provided and judged to be appropriate.
- **Para 47c**: while we appreciate the need to collect information that will eventually enable assessments of concentration to CSPs, we do not see how extending the full requirements of this section to all CSP outsourcings, regardless of whether they are critical or important, will always be relevant. This section should only apply to critical or important outsourcings. We understand that there may be underlying concerns regarding the ongoing assessment of materiality but note that these are already addressed through the other sections of the GLs and risk management processes in particular.

- **Para 47c v:** states that a register should include the date of last and next scheduled audit, where applicable. It should be clarified this specifically means external audit (as opposed to internal audit)
- **Para 47 c vi:** our members would welcome more information on what type of information should be provided with respect to the assessments of substitutability/reintegration – this may otherwise be difficult to provide in a register format
- **Para 47 c viii:** it is not clear what is meant by an outsourcing being "time critical"

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

Outsourcing of operational tasks associated with control functions and authorised activities

Para 49 b: The proposed switch to the concept of 'critical or important' outsourcings (rather than material outsourcings), for example in paragraphs 11 and 49, could result in an unnecessarily broad range of activities being subject to the greater requirements for critical or important arrangements. This goes beyond the MiFID approach by adding an additional trigger – whenever operational tasks of internal control functions are outsourced.

Accordingly, all outsourcings of the operational tasks associated with control functions would be deemed critical, whether they are or not in practice, with associated Key Performance Indicators (KPIs) or equivalent required as a consequence. Taking the ability to determine materiality here entirely out of the hands of the institutions would seem to de facto prevent the principle of proportionality from being applied in such case. We understand that this choice may be linked to concerns regarding so-called empty shells. We also fully recognise that authorised entities must have the appropriate oversight of their business and cannot outsource their responsibility. Nevertheless, we suggest that the blanket approach adopted in the GLs goes too far, and that room for respecting proportionality in cases that are clearly immaterial would help reduce the compliance burden currently associated with the draft GLs.

Para 49 c: The definition of 'critical or important' also includes the outsourcing of any banking or payment services subject to supervisory authorisation. As noted elsewhere in our response (see question 13) the requirement to inform regulators of planned critical or important outsourcings before actually committing to the activity creates significant business case risk.

Outsourcing of activities, processes or services related to core business lines and critical functions

Para 50: requires that all outsourcings regarding activities, processes or services relating to core business lines and critical functions should *always* be considered as critical or important for the purposes of the GLs, expanding the definition of 'critical or important' beyond what is in practice 'material'. For the sake of clarity, and to avoid an unnecessary broadening of the critical or important concept (and associated compliance and "supervisablity" burden), the wording "*relating to*" in the sentence "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" should be changed, for instance replacing it with the wording "directly applicable to" or "part of"". The choice of the wording is crucial as "relating to" means that *all* activities and processes potentially linked to core business lines or critical function would otherwise be considered as requiring inclusion with the risk that the number of critical /important activities to assess could dramatically increase.

Para 51: The criteria provided in this paragraph from g) to j) should be considered as information to be used for risk assessment purposes (Section 9.3) rather than as criteria for assessing the nature of outsourcing arrangements.

The term "conduct" (in paragraph 51.b.iii.) should be clarified as, among others, it could be related to customers, markets or employees.

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

Institutions can be in a comparatively weak negotiating position with respect to certain service providers, which may render compliance with the proposed requirements difficult in practice. A mechanism to reduce or share the burden of compliance would therefore be welcome and we strongly encourage the EBA and CAs to facilitate this, for instance by encouraging the creation of market provided quality labels or certifications as noted in our overarching comments

We also recall that a more pragmatic approach to sub-outsourcing needs to be adopted for this section of the GLs to be practicable and that, this section is not relevant with respect to intragroup arrangements (the governance set up for such arrangements is of course essential, but the requirements in this section are not relevant).,

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

We find this section of the GLs to be overly prescriptive and burdensome.

In relation to intragroup outsourcing, the application of concentration risk as a part of the risk assessment is inappropriate as the risks of a third-party outsourcing provider impacting on BAU operations is different to an intragroup service provider in resolution. As already mentioned, appropriate regard should be paid to both recovery and resolution plans and servicing arrangements for group-wide resolution instead.

Para 57: We have already commented on the need to restrict the specific risk assessment requirements in these GLs to outsourcing contracts rather than to make them generally applicable to all arrangements with all third parties

Para 59b: the requirement to assess the aggregate risks that may arise from outsourcing many functions across an organisation will already be dealt with via existing requirements for monitoring and managing operational risk. This should be reflected in the final GLs.

Section 9.3 poses particular difficulties in the context of sub-outsourcing. In practice, institutions are not likely to always have access to the information or the resources needed to address the potentially extremely high number of sub-outsourcers that could be implied by the draft GLs. This could be addressed by the EBA:

- Clarifying (i.e. restricting) the definition of outsourcing as already described, and therefore sub-outsourcing too
- Clarifying what is meant in **para 60** by the "service provider sub-outsources critical or important functions to other service providers", in a way that ensures an appropriate balance between the need for firms to consider material risks in sub-outsourcing cases together with the overarching principle of proportionality. This should also be considered and clarified in **para 61** so that is clear what is intended.
- Considering tools such as certifications, standards, etc. with other relevant authorities as required, to facilitate harmonised application of the GLs across institutions and the control of risk. This will also help reduce the costs and compliance burdens that could otherwise have negative effects on sound business cases for outsourcing

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?

Contractual phase

Para 63 e: this paragraph requires the specification of the location of data in the contractual phase. In practice this may be difficult at the early stages of the contractual phase. This could be the result of the design of a bespoke service which may not be fully developed at the time the two parties enter intro contractual negotiations. We recommend that it should be enough that the outsourcing institution maintain the right to specify the locations of data storage and processing throughout the life of the contract and that this cannot be changed by the service provider unilaterally.

Para 63: g and h – see comments on audit and access rights see below (para 72)

Para 64: requires, in the case of outsourcing of critical or important functions, that provisions should be clearly set out in the agreement to ensure (i) the access to data owned by the institution in case of insolvency of the provider (64. h) and (ii) in the event of insolvency or discontinuity, that the relevant data will be made available to the financial institutions (64. i). We note that it may be very difficult to exercise such rights as insolvency law can unilaterally change contracts or terminate them (under Italian law, for example, in case of insolvency of a provider, the contract is terminated by law unless the curator decides otherwise. Any conflicting contractual clause will be ineffective).

We note that such legal realities again point to the potential for the requirement of living wills mentioned in our overarching comments for data centres to address multiple regulatory concerns related to cloud outsourcing.

Sub-outsourcing of critical or important functions

Please also refer to our comments above on paras 60 and 61.

This section of the draft GLs is likely to be impracticable as institutions are unlikely to be able to obtain the relevant information or negotiate the type of contractual clauses described here. Moreover, this part of the GLs does not take into account the fact that the institution is engaged only with the main contractor and does not negotiate with sub-contractors. Cascading down regulatory requirements down the outsourcer's supplier chain may therefore not be a realistic objective.

We strongly encourage the use of alternative approaches to overcome these practical issues, such as allowing the institution to conduct an assessment of the main provider's third-party approval process. Moreover, for CSPs, reference to accepted standards such as ISO37500:2014 (which provides guidance on outsourcing process and governance) would facilitate the supervisory objective while at the same time helping reduce the friction between an institution and CSP. It would also provide consistency across the industry with respect to way the potential risks associated with chain outsourcing are addressed.

Para 66(b) does not work in practice. While we understand its underlying rationale, we feel it is largely duplicative with para 65. Again, it is unlikely that the institution will be able to achieve para 66(b) as it will not have a contractual relationship with the sub-contractor. An institution will only be able to seek an undertaking to that effect from the service provider.

Access, information and audit rights

This is another area of the GLs that creates significant business case risk and may call in doubt otherwise beneficial outsourcing arrangements. A clearer definition of outsourcing will assist in mitigating this issue and needs to be combined with a better delineation between what is required for critical or important outsourcing together with a more specific articulation of how the proportionality principle will function in practice. As drafted, this section will potentially make the execution of very simple outsourcings much more difficult.

We wish to draw to the EBA's attention that the access and information requirements applied to outsourcing arrangements will present issues where banks themselves act as an outsourcing provider to other banks. In many cases for trade reporting and data collection, allowing access to premises, systems and information for these services would be an unacceptable risk to information security and intellectual property. Rather than imposing these requirements, there should be a recognition that where outsourcing is provided by an institution subject to an equivalent or the same outsourcing regime, that they should be excluded from these requirements.

While fully accepting specificities of prudential supervision of the institutions in scope of these GLs, we would also encourage the EBA to reconsider this section generally using the lens of what supervisors themselves would deem to acceptable in terms of providing third parties access to the institutions they supervise.

Para 72: While we fully recognise the need for relevant access, information and audit rights to be in place we find the drafting of para 72 to be too broad for the purpose of providing the institution or the CA with the required access. For instance, para 72.b. refers to "unrestricted rights of inspection". We assume this is intended to be in the context of what is relevant to the outsourcing arrangement, but the use of the term "unrestricted" could be seen as being

excessive. Such language is likely to be unacceptable to many service providers. At the very least, access should be during business hours and at reasonable notice, but we suggest that for the purpose of the GLs reference to the "necessary rights of inspection" would be sufficient.

Alternatively, the EBA may start with a very broad general approach to access rights, but recognise that service providers will need reassurance that this will be done in a manner providing as much notice and visibility as possible, particularly in BAU cases. We recall that providing access to business premises may have limited practical benefits. Currently for security and resiliency purposes data may be held in various locations leveraging encryption and data partitioning techniques. Therefore, it may be sufficient to have physical access to the sites where the service provided is deemed most relevant to the regulated entity.

In general, further clarification is required regarding the terms "business premises", "reasonable time" and "due to an emergency or crisis" should be provided as these may create subjective and differing interpretations amongst CAs. Finally, the interaction of requirements for data protection, access to premises and information security access should be considered to ensure they do not create conflicting legal obligations for outsourcing providers.

Para 74 & 75: We welcome the recognition that firms can make use of third-party certifications, reports and pooled audits. To ensure proportionality and to reduce compliance burdens, we would welcome additional clarity on what is intended in practice by the last sentence of para 74 ("… should not rely *solely* on these"). For instance, recognised international standards and certifications should be sufficient to fulfil supervisory expectations in many cases.

Para 75 e and f: It is unlikely that a service provider will allow the inclusion of the contractual rights of such a potentially broad scope. Both points should be refined.

Para 76: the wording "where relevant" is key in this paragraph and third-party reports should be acceptable in terms of satisfying penetration testing requirements.

Termination rights

Para 81: in order to be less subjective, point d should refer to "the likelihood of significant breaches" instead of "weaknesses "in data security management

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

Para 85: The updating of risk assessments should be conducted at a frequency that is proportionate.

Para 88: we agree that actions should be taken in such circumstances, including termination, however we suggest that the wording "if necessary with immediate effect" be replaced with "including within as short a time frame as possible" to ensure there is no unintended consequence on operational resiliency.

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

As already mentioned, and to avoid unnecessary duplication of work, this section should include reference to firms' approved recovery and resolution plans in particular with respect to intragroup arrangements. It appears to be drafted in relation only to third-party arrangements and as such fails to recognise the benefits of firms' plans and strategies.

Para 90: requires that institutions can exit outsourcing "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".

According to the criteria given in section 9.1., critical outsourcing arrangements are precisely those that can impair the financial performance, soundness, continuity, […] of the institution. Therefore, we suggest that paragraph 90 should be amended to clarify that it only applies to critical outsourcing as follows:

"90. Institutions and payment institutions should ensure that they are able to exit **critical or important** 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: […]"

In addition, we would suggest simplifying the guidelines, which currently differentiate between exit plans and alternative solutions / transition plans. Generally, firms would expect simply to provide an exit plan to transfer to a new provider and an exit plan to transfer the service back in-house.

In the case of some cloud computing outsourcings there are two consideration involved in an exit, the service being provided, and the data being used to provide that service. In some cases, it may be more difficult to return the service than it is the data used to provide that service. In such cases, the outsourcing firm may prioritise ensuring that in the event of an exit caused by business continuity or other regulatory/risk-based concerns, the data is retrieved from the service provider such that it can be used to provide the same or equivalent service to customers. This is an important distinction as service offerings from cloud providers grow more unique and sophisticated making them harder to move between providers or back on premise.

In such cases we refer to our comments (see general comments above) on the potential benefits of living wills for data centres. We recommend the GLs include recognition of the difference between service and data in the context of exit planning as this will allow firms to better target their risk controls and plans toward the more "valuable" target.

Lastly, we feel it is important to stress the importance of the principle of proportionality with respect to expectations regarding tests of exit plans in practice and would welcome further discussion with the EBA as to how this is likely to work in a cost-efficient manner.

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.

Register

Please refer to our responses to questions 1 and 8 on the definition of outsourcing and the proposed content of the register respectively for suggestions on how to limit the information contained in the register to items that its content is proportionate and useful for supervisory purposes.

Additionally, more information on the "common data base format" that firms are expected to use for informing their supervisors is necessary (is this intended to be something else other than the excel spreadsheet provided as an annex to the consultation?).

Generally speaking, more time will be needed to build the register with all existing arrangements (i.e. longer than the proposed Dec 2020 deadline). We suggest this be extended to December 2021. To facilitate compliance, and to reduce the business case risk/uncertainty to firms during this period, we also suggest that during the proposed transitional phase that there should be no link with the power for the CA to terminate existing arrangements (under para 105).

Once the register is built and reaches a steady state, in order to keep the supervisory process manageable for both firms and supervisors, we recommend that register be made available at least every 3 years, rather than on an annual basis.

Notification

Para 93: Greater clarification over the timeline for the institution to inform the competent authority of planned outsourcing of critical/important functions is required as we understand this is an area where practice differs across Member States today. This also applies to the time line for communicating a change in an existing non-critical/non-important arrangement to a critical or important status (para 94). This time period is important as the notification requirement should not have an undue impact on the speed at which institutions can implement their decisions. Notification of critical or important outsourcing involving (changes to) sub-contractors is also particularly onerous/difficult to achieve in practice and may also create disincentives for firms' use of outsourcing and adoption of cloud technologies.

To avoid the considerable uncertainty created by para 93, and if there is no further specification of the context in which CAs might exercise their powers under para 105, the timing and type of notification should be an ex post notification (as it is clearly not an authorisation either).

We would therefore welcome clarification that this is an ex post notification rather than ex ante.

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

As noted previously, more information on how CAs will use the register in practice is required, and we would welcome inclusion in this Section of the GLs the requirement for CAs to detail what decisions they will make with the register, how it will be used, and what policies it will affect and to set their own risk appetite.

Para103: raises explicitly the issue of industry wide concentration risk. As noted in our introductory comments, the question of industry-wide concentration risk should be addressed by regulators in greater detail and with some urgency, in consultation with the industry.

Para 105: The EBA should be aware that, without additional clarity on the reasons for and process behind authorities requiring restrictions or exits from arrangements this section of the GLs create significant business case risk and prevent firms from entering into appropriate and otherwise beneficial outsourcing arrangements given the potential uncertainty they would face during a notification period.

We understand that termination of contracts should be rare but additional explanations of when this would occur would be helpful, as would the explicit statement that there would first be a process (possibly part of the routine supervisory dialogue) whereby supervisors would signal concerns, allow for mitigating actions in its compliance and governance programme, etc. before such a termination request would be issued.

The GLs should require CAs to set policies describing the steps in place to warn and monitor an outsourcing firm prior to the requirement to exit. These steps should be clearly defined and made public such that the outsourcing firms are able to ensure they take appropriate action. Finally, it should be recognised that regulators should expect firms to have effective monitoring and oversight such that a situation in which a firm is required to exit an outsourcing does not arise. Any requirement to exit an outsourcing contract by a CA should clearly be a last resort.

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

We have noted our general concerns regarding definitions above. In particular, the need to provide specific category names for the type of cloud outsourcing technology being used (e.g. "IaaS, PaaS, SaaS, public/private/hybrid/community") creates an unnecessary burden to continuously monitor and update a restricted list and is not "future proof". There are no agreed definitions for these terms and nor is such a definition desirable owing to the continuous evolution of the technology. Thus, any such requirement would lead to potentially overlapping or conflicting reporting as firms struggled to classify the technology into inappropriate categories. We fully recognise the need for authorities to collect information on concentration risk, particularly with CSPs. However, it is not clear how the use of such undefined categories in the template will assist in that objective. It is however likely to create significant compliance and monitoring burden and is one of the reasons for us suggesting that the register be built up with an initial focus on critical and important functions.

Global firms are spending increasing time debating the definition of fields of required information leading to significant duplication of work. Ultimately, as argued above, we believe this weakens the potential for a consistent and appropriate regulatory response and supervision. The EBA should encourage a programme of harmonisation of field definitions among CAs such that even if one CA should choose to require information in addition to another CA, the requirements will be consistent in definition between the two CAs. Ultimately, the answer may be found in machine readable regulation and text and we point to the work being progressed for instance by the FCA in this area as a model to emulate.

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

Please see above for the areas where our members are most concerned about the burdens and costs associated with these GLs.

AFME contact

Jacqueline Mills, jacqueline.mills@afme.eu +44 (0)20 3 828 2710

About AFME

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society. AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is listed on the EU Register of Interest Representatives, registration number 65110063986-76.