24 September 2018
EBF_033437

EBF comments on the draft EBA Guidelines on outsourcing

General comments and key points:

Outsourcing arrangements are widely used by the banking industry as they contribute to the efficiency and to the competitiveness of banks' business models. Outsourcing indeed helps banks focus on their core business and gives them access to skills and services that are not available in house at the same level of efficiency and/or effectiveness.

Against this background, it is crucial that the Guidelines (GLs) strike the right balance between necessary safeguards preserving the integrity of outsourcing institutions, and the required flexibility to adapt to a fast-moving economic and technological environment. In particular, we assume that the specific requirements (should) only apply to outsourcings classified as critical/important.

The EBF's key points relate to the following issues:

- **Scope of outsourcing**: The draft EBA GLs provide for outsourcing requirements that are in line with MiFID II. MiFID II only provides for requirements for the 'performance of operational functions which are critical for the provision of continuous and satisfactory services (…)'. It must also ensure that outsourcing of important operational functions is not undertaken in such a way as to impair materially the quality of its internal controls and the ability of its supervisor to monitor a firm's compliance with all its obligations. MiFID II does not provide for requirements on 'other outsourcing arrangements'. The scope is clearly limited to 'critical and important operational functions'. We therefore believe that there is no legal basis to develop guidelines relating to 'other outsourcing arrangements'. Moreover, the draft EBA GLs should take into account other existing regulations in matter of outsourcing (as Solvency II and PSD2) for consistency.
- **Definition and examples of what is or is not outsourcing:** The current definition is extremely broad and risks encapsulating all activities performed by third parties for regulated institutions as outsourcing. As there is no legal basis for such a broadening of scope, we consider that the GLs should be amended accordingly. Moreover, a process, a service or an activity should be qualified as outsourcing only where the service provider performs it on an ongoing basis. This condition should be included in the definition of outsourcing or specified by the EBA in the title II of these GLs ("Outsourcing arrangements"). The risk related to a short-lasting or "one-off" service should be limited. Finally, there are only a few examples listed in the draft EBA GLs of activities that are not considered outsourcing. The EBF considers that some more guidance would be very helpful – see our answer to Q1 below.
- **Intragroup outsourcing**: Intragroup outsourcing should be subject to lower obligations than extra-group third-party outsourcing agreements. The GLs should recognise 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

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

on documentation, due diligence, concentration risk and exit strategy prove to be less relevant from an intragroup perspective.

- **Standard contractual clauses will be necessary for outsourcing agreements**: Financial institutions may find difficulty in negotiating and getting some of the terms required by these GLs to be accepted by some large suppliers, such as, *inter alia*, the exercise of unrestricted access rights, or *ex ante* notification requirements in the sub-outsourcing of critical functions. 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 we believe that it would be positive in other contexts as well.
- **Sub-outsourcing assessment**: Institutions may find it difficult to perform the risk assessment of sub-outsourcing activities. This will not only depend on suppliers to inform about changes in their supply chain –information that has commercial value in itself and that not all service providers may always be willing to provide - but also on institutions being able to access and perform the due diligence of sub-service providers through the whole outsourcing chain, which potentially might be long. We propose the alternative that as part of the due diligence process of outsourcing providers, entities could analyse their provider's sub-outsourcing policies in order to guarantee an adequate control of their risks and service level agreements, instead of actually verifying full compliance by each sub-outsourced provider. This assessment should be based on an impact analysis on the outsourced services and related risks.
- **Notification requirements**: Given that the EBA has reiterated publicly that no upfront approval of outsourcing activities is necessary, in our view it would be sufficient for any bank to have a repository available which could be delivered upon request to the NCAs.
- **Summary table of requirements**: Across the GLs it is not clear which requirements apply to general outsourcing, which to outsourcing of a critical or important function and which to intragroup arrangements respectively. In order to provide clarity on which are the specific requirements for each type of outsourcing, it would be helpful to compile them all in a specific table or diagram to identify which are applicable to each service. At least, each chapter should clearly define for which kind of outsourcing is each rule applicable (please see our proposal in the Appendix).
- **Cloud**: The consideration of cloud services as outsourcing and, in case it is considered as such, as general outsourcing or outsourcing of critical functions should follow the same principles than the rest of services and technologies. It should depend on the nature of the activities outsourced.

Cost of implementation:

The EBF has consulted Members about the expected costs of implementation of these GLs. Considering the extremely broad definition of outsourcing as well a lack of proper limitation of all cumbersome requirements to critical/material outsourcing, it is expected that the initial implementing costs, as well as the permanent continuous costs will be significant. For instance:

- It is expected that the number of contracts considered non-critical/important falling within the scope of these new GLs will increase at least 100%, in comparison to the current CEBS GLs. While the number of contracts considered critical/important falling under scope of these new GLs will increase approximately at least 150%, in comparison to the current CEBS GLs. A number of existing non-material outsourcing contracts will become critical/important. In any case, it must be considered that the actual increase in number of contracts to be considered as outsourcing is directly related to the broadness of the definition of outsourcing that will be devised in the final GLs. Should the definition embrace most (even if not all) of the contracts for the procurement of services (including, e.g. maintenance of buildings, security of the premises, development of software, IT operations, consultancy services) the actual numbers could be very high. One of the major Eurozone banking groups has pointed out that the number of service contracts could reach thousands of new contracts per year (with most of these contracts consisting in "small tickets"). For each new contract, an additional effort involving the internal risk assessment functions (e.g.: legal, compliance, risk, privacy, information security, IT dept.) will be required. It is therefore crucial to clearly define outsourcing (even providing examples of activities non-relevant as outsourcing) and clearly distinguish outsourcing from procurement. In any case, considering the detail of the new GLs it is at least highly unlikely that any increment in number of contracts could be managed by existing internal structures.
- However, the number of additional contracts itself is not going to be the only driver of additional costs. What is much more critical is that the effort for cases that are deemed non-material today

will increase enormously as the GLs do not differentiate sufficiently between critical/important and non-critical/non-important cases.

- One small institution estimates expenses of about €1 million for re-designing their processes (excluding permanent costs related to staff necessary to ensure compliance).
- Another medium-size bank informed the EBF that it expects an impact of 8 FTE one-off for implementation and additional 27 FTE thereafter.
- Another large institution estimated that its set up cost could reach up to €1.4 million - €1.6 million. This includes tasks related to updating the current outsourcing framework (policy, handbook, procedures), review of arrangements to determine outsourcing versus not outsourcing and level of materiality, upgrade contracts and renegotiate, risk recertification, building of the register, review business continuity and exit plans, coordination, change management and training. It is estimated that its recurring costs would amount to an incremental €1.2 million - €1.4 million. This relates to efforts of business owners to monitor risks and performance levels, ensure business continuity testing, process due diligence requirements, governance time, support time.
- Another medium-size bank informed us that it will need a new and more specific internal database and reporting tool for outsourcing and it is expected that this will require 2 FTE on group level. In addition, the business and the control functions will be much more involved in the outsourcing files and according to its estimates an average of 3 to 4h/y for every file seems to be required. Considering that the current very wide definition of outsourcing is expected to capture a very large number of contracts, it is estimated that it will provoke at that bank some 24.000 extra man hours (or 16 FTE).

Other provisions of these GLs, as we detail in Q16, such as the risk assessment on each third party, the fact that intra and extra group are equivalent, or requirements regarding sub-outsourcing risk assessment and monitoring, could also trigger a relevant economic impact. In order to get a better idea of the expected impact that these GLs would have for financial institutions, we suggest that the EBA could perform an impact analysis to get quantitative evidence that could help better understand some of the issues raised in this response.

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?

General comments on Subject matter, scope and definitions

The EBA wants to align the definition of outsourcing provided in MifID II with the purposes of these GLs. However, it should be noted that the Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II (Delegated Regulation):

- regulates only "outsourcing of critical or important functions" (not establishing particular requirements in case of not critical/important outsourcing);
- clearly limits the outsourcing of critical or important functions by explicitly excluding from the scope of the MiFID II Regulation certain activities, such as the provision to the firms of advisory services, training, billing, premises security, market data/pricing services and the purchase of standardised services (see art. 30 par. 2, point a) and b))[1];
- defines outsourcing (art2 (3)) as: "arrangement of any form between an investment firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the investment firm itself", while the proposed definition of EBA GLs is actually broader since, after "by which that service provider performs a process, a service or an activity" it adds the words "or parts thereof" that can significantly broaden the definition. Aside from that, EBA also provides that it is not relevant for the outsourcing requirements whether or not the institution would be able to perform the function and/or operation itself which is not in line with art. 2 (3).

As the EBA GLs are not limited to such topics but also incorporate the general definition of outsourcing provided by the abovementioned Regulation, from the EBF's perspective, this will make it difficult to define the outsourcing scope and will create room for different interpretations, causing their application to become more complex/costly than it currently is, and what is necessary, in light of the EU Regulations in place. This in effect removes the stated goal of the revised GLs which is to harmonise regulatory practice across the EU.

In particular, without providing any criteria to bound outsourcing scope, and based on the EBA's proposal, especially wordings such as "any arrangements" and "that would otherwise be undertaken by the institution", one can interpret that all third-party arrangements can be considered outsourcing, except for the very few exemptions mentioned in paragraph 23.

As mentioned above, unlike the Delegated Regulation (see article 30), the draft GLs do not establish any connection between the definition of outsourcing and the regulated/core activities. Therefore, they mix different kinds of outsourcing activities:

[1] Moreover, we are of the opinion that at least most of such activities (in particular: "the provision to the firm of advisory services, and other services which do not form part of the investment business of the firm, including the provision of legal advice to the firm, the training of personnel of the firm …. and the security of the firm's premises and personnel"; as well as "the purchase of standardized services, including market information services and the provision of price feeds" can't be considered "outsourcing" per se (being mostly services typical of other business and in many cases – i.e. legal advice, security services … etc – being subject to authorizations or qualifications normally not in possession of banks.

- Activities under paragraph 23 of the GLs that normally are not performed by the institution and should not be regulated (conversely this means that if some acquisition of services, goods or utilities are normally performed by the institution it should be regarded as an outsourcing activity);
- Outsourcing of critical or important functions;
- Outsourcing to cloud service providers;
- Outsourcing arrangements that involve the handling or transfer of sensitive data;
- All other outsourcing arrangements.

Considering the above, there should be a clear and detailed EBA's interpretation of the applied outsourcing definition, in line with the MiFID II Regulation clarifying the elements that define outsourcing scope (see also recital 30 of the Rationale) and applied in a uniform way in all EU Member States. In particular, paragraph 17 of the draft GLs in the "Rationale and objective of the guidelines" chapter, should be implemented in light of:

(i) the contents;
(ii) the duration of the services provided by the third party.

Relating to the contents of the process, service or activity provided by the third party, the following are to be included in the outsourcing scope: "banking and financial services" which would be normally undertaken by the institution itself, according to its business model, including "Regulated Services or Activities", those relating to "core business lines and critical functions", as well as those processes, services or activities which are integral to their provision or aimed at supporting or controlling them. Insofar, Article 16 subs. 5 MiFID II, which is the basis for the outsourcing definition in Article 2 subs. 3 of the Delegated Regulation and ties the need for specific organisational outsourcing requirements clearly to "the performance of operational functions which are critical for the provision of continuous and satisfactory service to clients and the performance of investment activities", must be taken into account. The nexus to "banking and financial services" is therefore already implicitly part of the outsourcing definition in the Delegated Regulation and should be explicitly spelled out in the GLs for the sake of clarity.

As far as the duration of the service provision by the third party is concerned, in order to be considered as outsourcing, the process, service or activity has to be provided on an ongoing basis.

Finally, following the approach taken by the Monetary Authority of Singapore and the list of inclusions and exclusions included in their guidance, we urge the EBA to ensure that the list included in paragraph 23 is non-exhaustive and that it provides a more detailed list of examples in these GLs that are not considered as outsourcing, notably the following:

a. The full legal transfer of activities towards a third party, who subsequently acts in its own name and with own direct engagements towards clients;
b. The purchase of material goods, accessory to financial services (plastic (debit of credit) cards, card readers, authentication products, etc.);
c. Specifically, regulated activities and independent professional services, generally not compatible with the activity of the institution (such as, in most countries, the appeal to attorneys, notary practices, external auditors, medical professions, etc);
d. The supply of public/market data[2], including standardised data-research services which are available in the marketplace. Typical industry-shared arrangements, such as correspondent bank relationships; the use of technological platforms for

[2] See CEBS 2006-guideline 1.B

investment funds transaction(s); the purchase of services rendered by: monopolistic provider (or similar provider), State-owned provider or by Stock Exchange(s);

e. One-off/not recurrent services provisions/projects, i.e. the service will not be provided by the external provider on an ongoing or recurring basis but serves to deliver one single project;
f. Advisory services and other services which do not form part of the firm´s business and are typically offered by special professional groups, including the provision of legal advice to the firm, the training of personnel of the firm, billing services, the security of the firm's premises and personnel, advisory services by certified real estate experts or tax advisors;
g. Public services/infrastructures;
h. Agents/financial promoter services or collection of information (as considered a not banking normal distribution channel);
i. Standard ICT assets license agreement, software development agreement, supply of market/standard hardware, cloud platform or infrastructures as well as provision of maintenance services (both software and hardware) ancillary to the above-mentioned items;
j. Regulatory requirement to involve third parties, including rating agencies;
k. Recruitment and human resources support services (including payroll services), consultancy services, temporary staff supply or secondment, including, for avoidance of doubts, procurement of resources on a "time and material" basis;
l. Within a group, for example, central performance of certain functions provided by the parent company or other companies for the benefit of the group e.g. risk model developed from a parent group for all subsidiaries, supporting the subsidiaries with certain central liquidity management;
m. Real estate facility management and logistics, other Data Centers (e.g. general maintenance and cleaning, catering, transport, postal services, car management, travel management services, gardening procurement of basic services or products such as furniture and office supplies, printing, scanning and copying, public data transfer;
n. Agreements with third party providers for further education programs and training services for employees;
o. Involvement of credit intermediaries who only collect information from the customer and submit these to credit institutions to invite credit offers for the customer;
p. Public facilities (supply of electricity, water, gas, telephone and broadband) and the according ad-hoc operational assistance (this includes the provision of such services to (proprietary or rented) facilities of banks, similar to the 'infrastructure tenant' exception);
q. Procurement and development of general advertising campaigns and implementation strategies, event management, and market research;
r. Insurance services;
s. Sub-custodial arrangements;
t. Marketing & Communications: Paid Media (Advertising), Media Monitoring, Photography, Promotions & Offers, Public Relations, Sponsorship, digital marketing (social media, Text messaging, Electronic Direct Mail)
u. Professional Services related to travel: Accommodation (hotel), Transportation (air, ground, rail, water and other modes), travel management (travel security, travel tracking).
v. Support services provided by third parties on a partial component of the Information System for which the main phases of the IT process (in particular the architectural standards, change processes and business continuity / disaster recovery procedures) are under direct control of the bank.

In addition, cloud computing capabilities available to firms subject to these GLs for the key technologies of data processing, data storage, and networking, should not automatically be designated as outsourcing by default, particularly where there is no critical transactional activity managed by the third parties supporting the cloud infrastructure. It depends on the criticality of the supported activity.

The definition of "Sub-outsourcing" in the Definitions section should be further clarified by adding that this term is restricted to a sub-delegation of such activities (or parts thereof) that have been delegated to the service provider, and not such support that the service provider sources for its own infrastructure (i.e. IT desk top support that the provider has put in place independently of the outsourcing arrangement with the institution. We therefore propose to amend as follows:

> *"Sub-outsourcing means a situation where the service provider under an outsourcing arrangement further transfers a process, a service or an activity* ***delegated to him****, or parts thereof, to another service provider".*

Paragraph 5

We assume that in the context of these GLs there is no difference between "critical and important", thus only 2 categories are existing: "critical / important" and "non-critical / non-important". There are merely different designations in the referred EU Directives. The references are confusing, and the GLs should be clarified.

Paragraphs 12 & 13

The EBA has planned to apply the GLs from 30 June 2019 for new outsourcing arrangements. These new GLs require substantial changes in succession of process steps and the related internal policy framework as well as considerable staffing. In order to fully comply with the GLs - especially against the background of the principle of proportionality, which calls for comprehensive risk-mitigation measures for significant institutions (in terms of development of current procedures, necessary changes in used IT systems as well as amendment of outsourcing guidelines). Therefore, we recommend an extended deadline for implementation for new and existing outsourcings.

With respect to existing fixed-term outsourcing arrangements, these new GLs should apply at the renewal date following their entry into force (which could be in 5 to 10 years).

With respect to existing permanent contract, these new GLs should apply not later than 31 December 2022.

Paragraph 12 also requires making long-running contracts compliant with regulation at next renewal (which could be in 5 to 10 years), while paragraph 13 expects to have the register filled by the end of 2020, which then would lead to information missing due to not having renewed the contract (e.g. all details on sub-outsourcing). It should be clarified that for long-running contracts the requirement of paragraph 13 does not apply / applies only from the renewal.

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

In the absence of any waiver granted under the CRR or the CRD4, the GLs apply at group consolidated level and at solo level (i.e. the subsidiaries of a cross-border group must fulfil the requirements). Clarification is required (paragraphs 17 and 18) that the application of the GLs on sub-consolidated and consolidated basis is always restricted to licensed entities established in the EU in the financial sector to which possible statutory outsourcing provisions are applicable, otherwise the scope of application according to the GLs could go far beyond possible statutory regulations.

We note that Article 31.4 of the Commission Delegated Regulation 2017/565 specifies "*Where the investment firm and the service provider are members of the same group, the investment firm may, for the purposes of complying with this Article and Article 32, take into account the extent to which the firm controls the service provider or has the ability to influence its actions*". We consider that these GLs should take into account this article.

In the current draft, there is no preferential treatment of intragroup outsourcing. This contrasts with the fact that the EBA GLs on internal governance support group-wide integration, as requested by Article 109 subs. 2 of Directive 2013/36, and with the low-risk environment of intragroup outsourcing (largely comparable with in-house activities). We believe that the GLs should recognise:

1. the preferential status of intragroup outsourcing compared to the use of (external) third-party service providers, and;
2. 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 strategy prove to be less relevant from an intragroup perspective. Therefore, intragroup outsourcing should be subject to substantially lower compliance and reporting obligations than extra-group third party outsourcing agreements, as a service provider within a group entity is more closely controlled by the group that has the ability to influence its actions, notably for the control of the risks.

The GLs should take into account the specific case of the duty of oversight from the management body of the parent company on its affiliated companies. This should not fall under the proposed outsourcing framework. As an illustration, the parent company has the duty and the right to audit its affiliates, such duty and rights leading to reporting on these audits to the management body of these affiliates. The matter should not be seen the other way around, otherwise, if the affiliates outsource their internal audit to the parent company, it gives them the right to audit the parent company if they deem it relevant.

Moreover, extending the application of these GLs to institutions outside the EU could impact the ability to compete of those non-EU companies in their local markets, if local requirements on outsourcing are less strict than those set in these GLs, or even their ability to comply with regulations, if the requirements established in these GLs enter in conflict with requirements imposed by the competent non-EU authority.

The European competent authorities have diverse mechanisms, either multilateral, such as the college of supervisors, or bilateral such as the memorandum of understanding (MoUs) with authorities in third countries to guarantee the adequate supervision and identify weaknesses in the relationship and control procedures between the parent company and its subsidiaries.

Regarding the proportionality principle, we agree that some smaller institutions could find complying with these GLs challenging and require some flexibility. However, this principle should be applied in a way that does not confer any competitive advantage for those smaller institutions in the provision of a given service. Furthermore, we consider it to be of the upmost importance that compliance with these GLs does not influence any institution's competitive abilities and flexibility in executing its processes.

Finally, we would like to note that services agreements are required if a group member or certain assets and liabilities of a group are sold, in resolution or otherwise. Typically, the existing intragroup service agreements are terminated at the moment such a transaction is closed. These are replaced by a transitional services agreement between the seller and the buyer, under which the seller agrees to continue to provide services to the sold group member at the same level as before the sale, until the provision of the services is assumed by either the group member itself or the buyer. One of the reasons of having a specific transitional services agreement is that transitional services agreements may benefit from being VAT exempted. These transitional services agreements typically are far less complex than the sale and purchase agreements itself, they can be easily negotiated at the time of the transfer of the group member or the assets and liabilities. Typically, the buyer will require that the provision of services is continued, otherwise it may impact the value of the activities of the newly acquired group member. For that reason, already having intragroup outsourcing agreements in place does not seem required for situations in which a group member or certain assets and liabilities are divested, either as part of resolution or regular M&A activities.

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?

As mentioned in the introduction, requirements of these GLs are limited to supervised institutions. However, institutions do not always have sufficient bargaining power with large suppliers to include some of the clauses required, such as sub-outsourcing requirements. Therefore, in addition to the safeguards provided, we believe that to ensure effective supervision, these GLs should also apply to outsourcing providers, who should also facilitate compliance, and allow authorities to monitor their compliance. This is particularly necessary, for efficiency and soundness reasons, when outsourcing services are concentrated in one or a few dominant service providers in the financial sector which could become a single point of failure for the whole financial system.[3] In these cases, we believe that it would be preferable that authorities are able to monitor and certify the use of these suppliers for the outsourcing of activities by financial institutions.

[3] According to the EBA report on the prudential risks and opportunities arising for institutions from FinTech (July 2018), regarding to cloud outsourcing services "ICT outsourcing risk could be also considered important, not only from the point of view of individual institutions but also at an industry or systemic level, as large suppliers of cloud services could become a single point of failure should many institutions rely on them". The report highlights also the risk of concentration in a small number of market dominant providers when using other technologies such as biometrics, robo-advice services, or big data and machine learning. In the same line, the BCBS in the report Sound practices. Implications of fintech developments for banks and bank supervisors (February 2018) mentions that "the rise of fintech leads to more IT interdependencies between market players (banks, fintech and others) and market infrastructures, which could cause an IT risk event to escalate into a systemic crisis, particularly where services are concentrated in one or a few dominant players".

The EBA provides that it is not relevant for the outsourcing requirements whether or not the institution would be able to perform the function and/or operation itself. This is contradicting art. 2(3) of the Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II, which clearly provides that 'outsourcing means an arrangement of any form between an investment firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the investment firm itself'. This requirement means a huge shift in the scope of the draft EBA's GLs, as the CEBS GLs clearly state that 'outsourcing is an authorised entity's use of a third party ('the outsourcing provider') to perform activities that would normally be undertaken by the authorised entity, now or in the future'. We suggest EBA to refrain from adding additional criteria to outsourcing.

As mentioned above in answer to Q1, we urge the EBA to ensure that a list included in paragraph 23 is non-exhaustive and that it provides a more detailed list of examples of activities that are not considered as outsourcing.

Paragraphs 22 & 23

The last part of paragraph 22"... it is not relevant whether or not the institution ….it would be able to perform it by itself" is in contradiction with the definition provided in these GLs where it is written that "…a service or an activity, or parts thereof that would otherwise be undertaken by the institution … itself" and therefore should be amended.

Moreover, we propose the deletion in the paragraph 23 of the word "normally" (the acquisition of services ……..that are not normally performed…).

Paragraph 24

Regarding the assessment of third parties, paragraph 24 states that institutions need to assess risks posed by any third party. In addition, paragraph 22 of the background section states that institutions need to consider and manage risks also to services provided by third parties and not considered outsourcing or if considered outsourcing, not considered critical or important.

We feel that the scope of these GLs should be limited to agreements considered as critical and important outsourcing of operation functions and not to any other kind of agreements that will have to follow their corresponding precautions. Indeed, having to perform a thorough risk assessment of any third party would increase the compliance burden dramatically and could become an unachievable requirement even if, for example, only specialised providers, such as electricity suppliers or telecommunication companies have to be assessed.

Therefore, we ask the EBA to remove paragraph 22 of the background section and reword paragraph 24 of the GLs as follows:

> "24. The risks, including in particular the operational risks, of arrangements with third parties **that fall under the definition of outsourcing and are related to a licensed activity** should be assessed in line with paragraphs 53 and 55 and Section 9.3, taking into account the application of the proportionality principle as referred in Section 1.".

Paragraph 25

It should be clarified that this paragraph only refers to the authorised activity and not to back office or complementary activities related to it. Therefore, we propose the following amendment:

> "25. Without prejudice to the requirements within Title III, institutions and payment institutions should ensure that banking activities or payment services that require authorisation or registration by a competent authority in the Member State where they are authorised are only outsourced to a service provider located in the same Member State or in another Member State, if one of the following conditions is met:
>
> a. the service provider is authorised or registered by a competent authority to perform such banking activities or payment services; or
> b. the service provider is otherwise allowed to carry out those services or activities in accordance with the relevant national legal framework.
>
> ***This requirement is only applicable to the main activity and not to any ancillary task related to it, such as, but not limited to, reconciliation, accountancy or customer support***."

Paragraph 26

In accordance with this paragraph, banking activities subject to supervisory authorisation (i.e. part of the banking license) can be outsourced to a service provider located in another EU Member State only if this provider is duly authorised to perform such banking activity (paragraph 25). If the service provider is located in a third country, additional conditions must be met, notably the existence of MoUs between supervisors. According to such MoUs, EU supervisors should have access to any information relevant to perform their supervisory duties.

Further, the draft EBA GLs include several options that aim to ensure that effective supervision can be performed if outsourcing takes place to third countries:

a. The service provider is authorised and subject to supervision;
b. Requiring that the banking law in the third country is considered as equivalent (decided by European Commission (EC));
c. The existence of a cooperation requirement between the home competent authority and the third country to ensure in any case the access and audit rights etc.

Many outsourced services will never be authorised or be subject to supervision. In particular, IT providers (of various kinds) are not usually authorised or regulated. For this sole reason, this suggestion does not seem practical. One might also ask what kind of 'authorisation' or 'supervision' is adequate. Moreover, we understand that paragraph 26 applies specifically to the complete outsourcing of an authorised banking activity or payment services, and we suggest that this be explicitly mentioned in the final GLs.

The requirement that outsourcing to third countries is only allowed if the (banking) law in the relevant third country is considered equivalent by the EC also raises concerns. Processes in which the EC decides on equivalence are generally unpredictable and time-consuming and might even contain a political element. Furthermore, equivalence decisions can be withdrawn or amended by the EC at little or no notice, while there is no effective right of appeal against the determination of non-equivalence for a third country. Taking into account all these considerations, financial institutions cannot base business decisions to outsource certain activities to a third country, on equivalence decisions by the EC.

The option regarding the conclusion of cooperation agreements or MoUs between home authorities and third countries meets similar objections. For example: since the European Central Bank (ECB) became the home supervisor of significant banks in the Eurozone, the ECB has made it known that it has 'stepped in' existing MoUs between National Competent Authorities (NCAs) and third countries and is negotiating new MoUs at the same time. However, the ECB has not published a clear list of MoUs that are currently in force, and as a result banks do not know which agreements have been concluded and if so, what the content of the agreements is. Moreover, the ECB has communicated that it will only sign permanent MoUs if 'third-country equivalence' has been established. If MoUs are conditional on third-country equivalence decisions, the requirement that MoUs are in place before outsourcing to a third country can occur, meets the same objections as the requirement to have equivalence decisions in place. As MoUs can also be renegotiated or terminated if the participating supervisors decide to do so, financial institutions cannot reasonably take important and costly business decisions dependent on the authorities' will to conclude cooperation agreements.

In general, enough safeguards are already in place to be able to assess whether outsourcing is advisable, independent of whether the outsourcing takes place to EU countries or third countries. In the latter situation, the existence or not of a cooperation agreement between authorities cannot be a precondition. In short, institutions must retain an appropriate organisation to oversee and manage the relationship with the service provider and have control functions in place that manages the risks related to the outsourcing contracts and outsourced activities. Institutions must be able to insource any outsourced critical/important and licensed activities within an appropriate timeframe. Institutions must apply due diligence when outsourcing activities and the activities of the institution are to be appropriately executed and service level agreements are defined as part of the outsourcing contract.

The only additional safeguard that could be an option as regards outsourcing to third countries could be the requirement that outsourcing to a third country is not allowed if the particular non-EU jurisdiction is chosen solely for the purposes of evading stricter standards than in the EU (recital (16) and Article 13 CRD).

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

Even though paragraphs 28 and 30(c) are not in Section 4, we would like to have the possibility to comment on them.

Paragraph 28

In case of intragroup outsourcing by multiple subsidiaries to an internal service provider, who is then considered to be the "management body", e.g. with regard to the resolution of conflicts of interest? In particular, in case of chain outsourcing by multiple subsidiaries to an internal service provider, who subsequently outsources the services to an external service provider, conflicting requirements (arising from local variations in requirements, risk appetite and controls) may arise. Who will be responsible and mandated to align these requirements at a principal level?

Paragraph 30

Sub-paragraph 30.c imposes a requirement to "establish an outsourcing function or designate a senior staff member (e.g. Key Function Holders) who is directly accountable to the management body or at least ensure a clear division of task and responsibilities for the monitoring of outsourcing arrangement".

The creation and follow-up of an outsourcing arrangement is in first instance the Process Owner's responsibility. We are of the opinion that different equivalent outsourcing governance models are possible (centralised in a specialised department, embedded in the concerned business, etc.). The institution's control departments are competent to verify the accuracy of the applied process. Therefore, the decision of establishing an "outsourcing function" should be left to the institution's decision.

Paragraph 31

Institutions and payment institutions should maintain at all times a sufficient retained organisation and not be "empty shells" or "letter-box entities". But clarification is needed in the GLs to know what minimum level is required for not being considered as « empty shells » or « letter-box entities ».

Paragraph 32

With regard to sub-paragraph (g), we would like to note that in certain cases, it is not possible to meet the requirement of identifying alternative solutions as part of the exit strategy, as no credible alternatives are available in the market. Not being able to identify any alternative solutions should not lead to a situation where outsourcing becomes impossible.

With regard to sub-paragraph (h) we note that compliance with the GDPR is already required pursuant to the GDPR and subject to supervision by the data protection authorities empowered to apply appropriate sanctions in case of violation. Therefore, we do not see the added value of adding an additional requirement for institutions to comply with the GDPR in these GLs. In addition, this may lead to conflicting guidance provided by supervisory authorities, which leads to legal uncertainty.

Paragraph 33

Clarification is required that the application of the GLs on sub-consolidated and consolidated basis is always restricted to licensed entities established in the EU in the financial sector to which possible statutory outsourcing provisions are applicable, otherwise the scope of application according to the GLs could go far beyond possible statutory regulations (see also comment to Q2, section 1 above). Therefore, it should be clearly stated that this policy is not to be implemented in those entities of the group being (i) licensed entities in the financial sector not located in EU Member States; and (ii) non-licensed entities in the financial sector.

Paragraph 34

Concerning Section 4, and especially paragraph 34, we are of the view that some of the requirements are too detailed for such a policy document adopted by the management body. For instance, paragraph 34(e) concerning exit strategies and termination processes, should instead be included in lower corporate level documents such as internal GLs and/or handbooks as it is too detailed for a high-level document. However, if the EBA decides to retain it, paragraph 34(c)(ii) should clarify that changes should be communicated if having relevant impacts on the outsourcing management. Therefore, clarification is needed to establish that all requirements included in Point 4 (Outsourcing Policy) must be addressed

either through the policy to be approved by the management body or through any internal rules and regulations of the entities developing and implementing such policy.

Also, complying with requirement in paragraph 34.b.v ("procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with Section 5") could be burdensome if any minor conflict of interests with third parties has to be identified.

Paragraph 35

The objective of differentiating between the listed type of outsourcing is not clear. What is the added value of having such requirement? Paragraph 35 states that the outsourcing policy should differentiate between the listed type of outsourcing (a, b, c and d): we deem that criteria used to distinguish the different type of outsourcing should be clearly identified. It is also necessary to understand if (and to what extent) could the policy differentiate such types of outsourcing. Insofar, we refer to our repeated requests in this document to more clearly distinguish in the GLs themselves between critical/important and non-critical/important outsourcing (see e.g. our comments to paragraphs 43, 45, 46 or 52 below) as well as between intragroup and external outsourcing (see e.g. our comments to Q 2 above). Without a much clearer distinction in the GLs and preferential treatment of non-critical/important and intragroup outsourcing, most distinctions in the internal policies will have no sufficiently solid basis in the GLs.

Moreover, in relation to group composition, it is unclear whether outsourcing of activities by an institution to a service provider which is member of the same group, but not controlled by the institution itself, qualifies as "intragroup outsourcing" arrangement and will be administrated / managed in the same way. E.g. paragraph 19(a) refers to "outsourcing arrangements with service providers within the group or …..", the paragraph 47(b.iv) refers to "institution's group" and 48(f) foresees that it has to be considered whether the service provider is part of the "institution's accounting consolidation group" …… -> these definitions are slightly deviating 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 dealt as outsourcing within the "institutions accounting consolidation group".

In addition, it is not clear what is meant by 'outsourcing to service providers which are authorised by a competent authority and those who are not'. Many outsourced services will never be authorised or subject to supervision. In particular, IT services (of various kinds) are not usually authorised or regulated. For this sole reason, this suggestion does not seem practical. One might also ask what kind of 'authorisation' or 'supervision' is adequate.

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

Consideration should be given to where EU banks act as outsourcing providers to other EU banks. EU banks will often provide trade reporting and data collection services and following the draft GLs would allow other banks access to premises, systems and bank information to an extent that these GLs would become an unacceptable risk and an extension beyond current access arrangements. There should be a recognition that the nature of the counterparties requires a different approach to the EBA outsourcing GLs to avoid these risks.

Paragraph 38

We would greatly appreciate clarification of what is considered "a material conflict of interests" as well as "sufficient level of objectivity" in this paragraph.

Paragraph 40

The requirements in this paragraph are not sufficiently clear. Although we understand that institutions need to have an appropriate Business Continuity Management Plan (BC plan) in place for critical or important functions, it is not clear whether institutions would need to know if the provider should also have a BC plan in place and whether the institution receiving their services should know it and/or accept it. Moreover, we would greatly appreciate clarification of what is considered "severe business disruption" in this paragraph and that a case by case analysis, depending on the risk exposure, is possible.

Furthermore, the EBA seems to be focused exclusively on the integration of the BC plan of the bank in the presence of suppliers/outsourcers. The EBA should clarify if it is acceptable and relevant to include in the outsourcing contract:

- clauses specifying BC requirements and requiring the BC plans or self-assessment questionnaires of the suppliers so that the service level in case of crisis and the BC solution adopted by the service providers are formalised in line with the business objectives and coherently with the prescriptions of the GLs;
- methods of participation, directly or through user committees, for the verification of suppliers' business continuity plans, also acquiring the BC plans of the supplier or adequate information about that, for the evaluation of the quality of the measures provided in order to integrate them with the continuity solution implemented internally.

Paragraph 42 et. al. (internal audit function)

Concerning internal audit function, and particularly paragraph 42, we believe the coverage of outsourced activities review, including on-site visits, performed under audit rights enforcements, should be set at an institution level and should be performed, under a risk-based approach plan, undertaken either by the second line of defence, specialised functions (IT, facilities, legal, compliance, etc.), internal audit function, outsourced specialists (third-party certifications, external auditors, etc.) or a combination of the above.

This supports a wider and more efficient review of outsourcing activities, ensuring that the audit rights are in place and can be effectively enforced (Section 10.3).

Internal Audit stands as third line of defence, being essential the role developed under a risk-based wide coverage on outsourcing arrangements, that should include visits to critical and important service providers, when considered necessary to ensure at least, but not only, the objectives set by the GLs.

Even so, Internal Audit should not substitute first or second line responsibilities or capacity, regarding third-party risk management, including the performance (when considered necessary) of independent on-site reviews to providers, related to, but not only, appropriateness of data protection measures, controls, risk management and business continuity measures, implemented by the service provider. In this way, sharing the role among the three lines of defence will increase the efficiency and eventually improve coverage of onsite visits thanks to a wider control environment.

Moreover, relating to Internal Audit activities, some clarifications should be provided on how to manage differences arising vis-a-vis the current local regulatory rules. In this

respect, the following relevant topics have been identified: (i) no periodical reporting to ECB on outsourcing matters seems to be required (while it is currently imperative for some regulators, even including the EBA as a recipient); (ii) how to reconcile the outsourcing risk categories proposed by the EBA (critical, important, others) with those currently set by local regulators.

Furthermore, it is suggested to specify the role of Internal Audit function as "support" in the definition of access/audit rights included in the outsourcing agreement.

In terms of auditing we would encourage the EBA to use its own recommendations on outsourcing to cloud services providers as a reference, which was very helpful for entities, and allow that they could rely not only on their own staff but also on certifications or pool of auditors, especially in the case of complex technologies. We suggest keeping this recommendation with small adjustments:

> "~~*Considering that cloud*~~ ***For*** *solutions* ***that*** *have a high level of technical complexity, the outsourcing institution should verify that the staff performing the audit – being its internal auditors or the pool of auditors acting on its behalf, or the* ~~*cloud*~~ *service provider's appointed auditors – or, as appropriate, the staff reviewing the third-party certification or service provider's audit reports have acquired the right skills and knowledge to perform effective and relevant audits and/or assessments of* ~~*cloud*~~ ***these*** *solutions"*.

Paragraph 43

As this clause specifies audit tasks as required in Chapter 10.3, we suggest deleting "in particular". It should be applicable only to critical or important functions, as otherwise all contracts would require full audit rights, requiring additional effort especially for subsidiaries outside the EU, where this clause is not common.

Paragraph 44

We suggest substituting the wording "ascertain" with "assure" for alignment to the International Professional Practice Framework (IPPF).

In relation to point 44.d, we suggest excluding the specific reference to "risk appetite, risk management and control procedure of the service provider related to the outsourced services" as the Audit function of the service recipient cannot cover the entire risk appetite, risk management and control procedure of the service provider.

Finally, we would like to ask whether the findings and recommendations regarding outsourcing arrangements to be subject to a formal follow-up procedure are only those issued by the Internal Audit function of the institutions and payment institutions.

As a general comment, clarification would be necessary on which requirements for BC plans, conflict of interest and internal audit functions apply specifically to the outsourcing of critical or important functions, which to general outsourcing, and which to intragroup arrangements respectively. In order to provide clarity on the specific requirements for each type of outsourcing, we would suggest having them all compiled in a specific table or diagram to identify which are applicable to each kind of outsourcing. We provide a suggestion of a table in the appendix of this document.

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

It seems inappropriate to require 1) in a unique register information that is referred at least to two different objects: Outsourcing Providers and Outsourcing Contracts, plus a sub-object relating to sub-outsourcing contracts identification 2) in a unique record-field information that can be only provided within the contracts/SMA or within other complex documents and not in a DB/Register format. Among these are the following: "47.a.iii" referred to the "reason why" the outsourcing contract has been assessed as "critical or important" (such information is not included in the example made in Annex I); item "47.c.v." referred to the result of Internal Audit inspection. All in all, it is suggested to require having in a table the key data necessary to identify each object (Provider or contract) and to guide the authority in accessing more detailed information made available in the information system of the institution.

Moreover, we consider that the creation of a customised IT-tool (the register), in particular in the context of an international banking group, will require substantial financial and human resources, in particular in order to keep it up to date. This cannot be set up in a couple of months. We believe that such work requires at least 12 months to have such a tool available, with additional 12 months to have the requested information on all existing outsourcing files available in the register. As a consequence, an initial application date for this requirement should be 1 January 2022 and limited to outsourcing of critical or important functions, for the implementation and initialisation phases.

Finally, we fully disagree with the cost-benefit analysis of EBA in p.59-60. By using a very broad and vague definition of outsourcing, and additionally requiring detailed registration, the EBA will create substantial additional work (=several FTE), with no or very limited additional value. The EBA is correct when it argues that information on outsourcing files should already be available for governance purposes / general management supervision; but this does not exist in the form and to the extent the EBA has in mind. The EBA proposal will result in the necessity to duplicate and combine different existing reporting tools. Additionally, the requested information on outsourcing providers is however completely new.

Moreover, considering the importance of the principle of proportionality, we suggest that reporting requirements should be limited to critical and important outsourcing towards external parties (not intragroup). This would reduce the extra work to a more acceptable level and keep more oversight for the supervisor. Critical and important outsourcing are the files that are sensitive from an operational risk point of view, and where the dependency risk on monopolistic service providers has relevance.

Finally, we also notice that the terms "arrangement" and "agreement and contracts" are mixed along the GLs and therefore it is not always clear what these terms refer to. Consequently, we request the EBA to use these terms more consistently and provide a definition for each one in the Definitions Section.

Paragraph 46

The scope of the register should be limited to critical and important functions only. Please further specify what type of subsidiaries should be subject to the overall register at institution and group level. We recommend focussing on subsidiaries considered on a risk-based approach. Furthermore, we suggest excluding sub-paragraph 47.c.v-x for intragroup outsourcings.

Paragraph 47

The requirement in paragraph 47.a.v. of keeping a record of the institutions within the scope of prudential consolidation that make use of the outsourcing agreement is not clear. We are inclined to understand that in this case agreement is equivalent to contract and, therefore, when each institution within the scope of prudential consolidation has its own contract with the provider, only that institution will be identified as user of that agreement.

Assuming that this interpretation is correct, we ask the EBA to reword this requirement as follows:

> "the institutions and other entities within the scope of prudential consolidation **that are covered by the outsourcing contract and make use of the services agreed in it**, including their names;"

With reference to the documentation and information to be maintained, we feel that these GLs are too prescriptive. We would like to make the following comments:

- The date of the last risk assessment and a brief summary of the main results (paragraph 47.c.i) should not be required. The brief summary is redundant with other information already maintained in the register, such as the function that has been outsourced and its consideration as critical. Moreover, the GLs do not set any time requirement for reassessing the risks of a provider and therefore, there appears to be no justification to have to keep the date of the last risk assessment in the register.
- Requiring Information on functions outsourced to cloud service providers, even though the outsourced function is not critical (paragraph 47.c.), is against the principle of technology neutrality and increases the compliance burden of cloud services before other traditional (not necessary less risky) technologies. Therefore, we request the EBA to remove the last part of paragraph 47 c ("and outsourcing to cloud service providers"). Documentation requirements for outsourcing to the cloud should be based on the nature of the outsourced activity, and the assessment of criticality or importance according to section 9.1.
  It seems that this approach is related to the statement in paragraph 43 of the background section ("although cloud services can offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost effectiveness, they also raise challenges in terms of data protection and location, security issues and concentration risk, not only from the point of view of individual institutions, but also at industry level"). However, we believe that the referred challenges depend on the specificities of the institution, cloud provider and service to be implemented. Therefore, we ask the EBA to remove this statement.
- Considering that these requirements include data that can change from year to year, we suggest either deleting sub-paragraph 47.c.x., or rewording it as follows: *"the estimated yearly budget cost as estimated at the approval of the outsourcing arrangement"*, to avoid at least a yearly update for every critical or important outsourcing contract.
- To be able to comply with the requirement in paragraph 47.c.viii., a definition and criteria on what "time critical" means are needed.

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

Due to the unclear definition of outsourcing (see our answer to Q1), it makes it difficult to evaluate the assessment of criticality and/or importance of outsourced functions – especially as there are so many parameters to take into consideration. In the cloud Recommendations there are only five parameters to take into consideration, this is a substantial increase which widens the scope for discrepancy.

Outsourcing of operational tasks of the internal control functions is considered critical or important as such without a materiality assessment. MiFID II states that an operational function (any processes, services or activities, or parts thereof) shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities. The draft EBA GLs seem more stringent than MiFID II on which paragraph 49 is based (see footnote 11 and text box on page 17), as MiFID II does include (the possibility of) a materiality assessment and paragraph 49 does not include such condition. We suggest the EBA to include same wording as in clause 30 of Regulation 2017/565 for outsourcing of operational tasks of the internal control functions, so as to have consistency in the wording and to avoid that outsourcing of every part of operational tasks of the internal control functions is considered critical or important.

The GLs would gain clarity if the different outsourcing arrangements would be described earlier in the document. We therefore think that Section "Title IV Outsourcing process" and especially Section "9.1 Assessment of the criticality and importance" should be moved to part "*2. Subject matter, scope and definitions*" which referred to "critical or important function" definition. Further, the definition of critical and important functions/processes and other outsourcing arrangements (paragraph 35.a) should be coordinated with the ECBs SREP to avoid two definitions of the same function. We also strongly suggest a transversal approach with ESMA and EIOPA, as the same concepts are used within their competence, and otherwise misunderstandings and reporting conflicts within (mixed) financial holdings can arise.

In relation to cloud outsourcing, as stated in Q1, outsourcing to cloud should therefore not be necessarily considered a case of outsourcing nor treated as a case of outsourcing of critical functions (such as it is suggested in the case of documentation requirements). This should depend on the nature of the activities outsourced according to the outsourcing definition, and to the assessment of the criticality or importance according to criteria set in section 9.1.

Paragraphs 49 & 50

Paragraphs 49.b, c and 50 should be redrafted so that the outsourcing of mere (subordinate) parts of banking services (or operational tasks of internal control functions or core business lines and critical functions) does not automatically entail the assessment of critical or important, but instead, that the materiality of the outsourcing of these activities is assessed using the other criteria (as set out in par 51).

Moreover, for the sake of clarity, with respect to paragraph 50 we suggest deleting 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". Such a deletion is crucial as the said

provision could mean that all activities and processes potentially linked to ("relating to") core business lines are to be considered included in the definition (even if consisting in mere technical support or standard devices). The risk is that the number of critical /important activities to assess could dramatically increase.

Therefore, we suggest amending this paragraph accordingly:

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

Finally, there seems to be a typographical error in paragraph 50: "using the criteria in Articles 7 and 8 of Commission Delegated Regulation 2016/778". The reference should be to Articles 6 and 7 (not 8 which is date of the entry into force).

Paragraph 51

We suggest moving this paragraph to the Section 9.3 "Risk assessment of outsourcing arrangements" as criteria mentioned in this paragraph are related to the risk assessment of the service and not of assessment of the critical or importance aspect.

In line with the remarks on the previous paragraph, we suggest that the wording in paragraph 51 indent "a)" "is directly connected to" is changed to "is part of".

In relation to paragraph 51.e, we ask the EBA to explain how can aggregated exposure or cumulative impact be measured/weighted by institutions.

We deem that the criteria in indents g) to j) should be considered as information to be used for risk assessment purposes rather than criteria for assessing outsourcing arrangements.

With reference to paragraph 51.b.iii., the meaning of the term "conduct" should be clarified as, among others, it could be related to customers, capital markets or employees.

Fulfilling the requirement in paragraph 51.e. is not feasible on group consolidated level: If there are several small outsourcings all non-critical or important for each Group Entity, the overall outcome should not be "critical or important".

Moreover, clarification would be welcome on how the criteria should play a role in order to assess whether an outsourcing arrangement should be considered as critical. In particular, we ask clarification as to if the consideration would be triggered by compliance with one only criterion or if there should be an amount of them at the same time.

Finally, relating paragraph 51.c.iii, clarification is needed about how the potential impact of the proposed outsourcing arrangement on the ability to conduct audits (regarding the outsourcing arrangement) has to be evaluated in coordination with the requirements

included in paragraphs 42 and 43 on Internal Audit activities and paragraphs 72 and 73 on Audit rights.

Paragraph 52

Regarding the substitutability of an outsourcing agreement, the requirement to assess the impact of a disruption of the service should be restricted to critical or important outsourcing arrangements that are the only ones that can represent a risk for the financial performance of an institution. Therefore, we request the EBA to reword the paragraph 52 as follows:

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

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

As we stated previously, the due diligence process is becoming problematic in some cases, where providers do not really understand the need to provide the information of such nature and quantity as required by the GLs. According to these GLs, every institution will have to perform its own due diligence of these providers separately. This is clearly inefficient for entities and does not necessarily ensure the best monitoring of risks by financial supervisors.

We have already suggested that authorities take a role by monitoring those providers that are used by a significant number of financial service providers[4].

In parallel, the EBA could explore the possibility to issue certification schemes, in line with the works of the European Commission Working Group on *Cloud security certification scheme*, but which are specifically applicable to the financial sector. This would also increase the efficiency of the process.

Paragraph 54

It needs to be clarified which kind of controls on the "financial situation" are requested when conducting the due diligence procedure and under which specific circumstances the specification "if applicable, group structure" applies.

Moreover, we need confirmation that analysis of the financial statement and control of the balance sheet are adequate measures when assessing service providers (and sub-providers, when it is the case). We would like to raise the awareness of the EBA to the fact that it is very problematic for institutions to obtain the balance sheets and financial statement of suppliers and third parties when their legal address is abroad. We therefore ask the EBA to take this issue into account when finalising these GLs.

4 This strategy has been followed by Authorities in other contexts. In capital markets for example, the regulation on the use of benchmarks initially required each institution to carry out its own due diligence of each index before using it. Given the inefficiencies associated with this process, benchmarks are currently certified by the European Commission. The same strategy applies for example to the use of Central Counterparties (CCPs).

The described due diligence assessment is very detailed and specific. We would wish verification whether the requirements are subject to the principle of proportionality and clarification if there is a difference between the due diligence assessment requirements regarding critical/important and non-critical/non-important outsourcing activities or not.

Paragraph 56

While the intention to ensure compliance with values and codes of conduct is welcome, we consider that this objective would be more effective if dealt with outside of these GLs, e.g. within GLs on internal governance or the general, non-banking specific corporate social responsibility framework. Though at times the industry falls short, the last decade has seen a renewed and concerted drive on the part of the banks to behave as good corporate citizens including through policies for procurement of goods and services in a socially responsible manner. Consequently, this paragraph should be removed.

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

Main Service Providers (specially IT providers) have a business model which includes continuous 24hr a day, 7 days a week service provision and this implies that they have a very wide chain of subcontractors in many countries. For many of them it is not possible or practical to provide information to the outsourcing institution about the sub-contractors in place at any time and nor would it be possible for their business model to give the veto right or the termination right because of a change or new appointment of a subcontractor. Furthermore, it is often impossible for them to accept in the outsourcing agreement the right to effectively supervise subcontractors by the outsourcing institution or by regulators. This is usually a non-negotiable position, which can create difficulties for the outsourcing institution, as the provider could be the only convenient provider from an economic or internal management point of view. In other cases, even if financial institutions could effectively negotiate the inclusion of such clauses in their outsourcing agreements, we cannot ensure that those service providers will be able to impose such conditions on their subcontractors, across the whole sub-outsourcing chain.

The EBF agrees that institutions should remain responsible for all outsourced activities set in the outsourcing agreement. However, we also believe that the outsourcing agreement should give to institutions which decide to outsource any activities at least the right to be informed by the third party to which the activity is outsourced of sub-outsourcing, and the right to resign from the contract in case the envisaged sub-outsourcer is not considered adequate.

The definition of sub-outsourcing should not include those cases in which the main service provider delegates a part of the service or contract any good, tool or license with a third party, 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 therefore be discharged from the obligations to those situations, due to the complexity to control them as a practical matter.

Paragraph 57

The reference in this paragraph to " … third parties, regardless of whether or not those arrangements are considered outsourcing arrangements" seems not appropriate. These GLs should be focused on outsourcing arrangements only; moreover, this general principle is already included in the regulation on governance and thus does not need to be recalled

here while assigning tasks related to non-outsourcing agreements. Requiring all third-party contract risk assessments to be documented would constitute an undue burden for the institutions, in light of the proportionality principle.

Paragraph 58

The draft GLs require banks to perform a scenario analysis on their operational risk for each outsourcing arrangement, where scenarios of possible risk events should be considered. We believe that this requirement is too prescriptive and that it should be instead outcome-based. Banks should be allowed to apply their own risk assessment approach provided it meets the objectives of the regulation.

Paragraph 59

In addition to the use of own risk assessment approaches (refer to comments above), there should be noted, that concentration risk assessments and mitigation actions are only reasonably possible on portfolio level and not as required in paragraph 59 (and others) on the level of the single outsourcing contract. Especially in a group consolidated view, there are many possible interconnections to consider after outsourcing activities, which cannot be reflected in each already existing contract.

Regarding the question of step-in risk, regulators should consider the benefits of requiring separate living wills for CSP data centres. Not only financial services, but a number of critical sectors are becoming increasingly reliant on cloud computing provided by one of the three main CSPs. Addressing concerns around step-in risk will thus be of benefit to many industries and could also help address concentration risk concerns by helping to mitigate against severe service failure affecting multiple organisations.

Paragraph 61

The meaning of "sensitivity" in paragraph 61.a should be clarified.

Please also clarify whose "oversight limitations" are meant in paragraph 61.c.

The requirements in Sub-paragraph 61.d appear "over-engineered", especially item iii. relating to insolvency laws. Implementing items i. to iii. in detail would lead to significant cost for legal advice. The degree of due diligence on foreign laws should be more left to the institution's discretion and risk-appetite.

Sub-paragraph 61.e should be applied to outsourcings to cloud or ICT outsourcing only, as it refers explicitly to data handling as it is typically for datacentre-related services. For Business Process Outsourcings those topics are normally not agreed in contracts as they are outcome based and not transactional.

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?

The EBA provided a substantial support to entities regarding the inclusion of contractual clauses by banks concerning access and audit rights when it issued its Recommendations on outsourcing to cloud service providers. We believe the current GLs under consultation could be a good opportunity to integrate the CSP provisions already in force without changes to their substance, reinforce those rights and extend them beyond cloud service

providers. Without this, there would be a different regime between outsourcing to the cloud and general outsourcing that we believe is not appropriate.

In general, it seems necessary to better clarify which requirements should be limited to outsourcings assessed as critical or important and not applied to other outsourcing agreements.

Furthermore, we take note that in case of outsourcing agreements (even in case of outsourcing of critical or important functions) service providers should grant financial institutions and their competent authorities unrestricted rights of information, audit, and access. As already foreseen by the EBA Recommendations on cloud, it is possible to use third-party certification and third-party reports even though they should not rely solely on those. Furthermore, it is also possible to use pooled audits organised jointly under specific conditions and the institutions shall always retain the contractual right to perform individual audits at their discretion. Finally, it should be clarified, that it is also possible that the audit function of the service provider itself can perform the audit, provided that the service provider has its own banking licence and thus can ensure an own audit according to banking standards.

The exercise of the unrestricted access right is very problematic too because, for example, service providers must grant the protection of all their customer data. The EBA GLs should aim at securing the necessary rights to ensure effective supervision of the service provider.

The interaction of requirements for data protection, premises and information security and outsourcing access should be considered to ensure conflicting legal obligations are resolvable for outsourcing counterparties.

Paragraph 63

As generally stated, we understand that specific requirements of the GLs apply to critical/important outsourcings only. Otherwise we consider requirements as outlined in paragraph 63 for non-critical and non-important outsourcings as too ambitious and not practice-oriented (e.g. agreement on comprehensive information, audit and access rights). We recommend focussing consistently on "critical or important" outsourcings.

The meaning of sub-paragraph "d" should be clarified, and in particular the statement " whether the sub-outsourcing of a critical or important function is permitted (…)".

In relation to the requirements that "the location of processing and access rights for institutions and competent authorities" is provided, we would like to observe that in cloud environments establishing the exact location of processing reduces the advantages of this technology paradigm that allows relocating or including new processing centres without impact on the service. Therefore, instead of "the location of processing", institutions should only be required to set "the region, country or countries where data are processed, transferred, stored, replicated, archived".

Paragraph 64

Concerning paragraph 64.c we consider it to be an institutions prerogative to make individual arrangements on reporting obligations. Therefore, we suggest the following rewording:

> "c. the specific reporting obligations of the service provider to the institution."

Regarding paragraph 64.f we need clarification on who should provide the business contingency plans: the service provider or the institution. In our understanding, the bank must have a BC plan, while the supplier must have a technical contingency plan. Accordingly, the requirement has to be requested by the customer to the provider; so, it is the service provider that has to implement and test the contingency plan, while the customer has to require to do it.

In sub-paragraphs 64.h and 64.i we would like to have clarification on the definition of insolvency for this purpose. Does it include the situation of resolution or deterioration of financial circumstances?

Moreover, in paragraph 64.i, in the case of outsourcing of critical or important functions, provisions should be clearly set out in the agreement that 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 both rights as insolvency law can unilaterally change the contract in course or make it cease, if the curator decides so. Under local laws, in case of insolvency of a provider the consequences may be different. Certain laws require the termination of the contract by law unless the curator decides otherwise. In other laws, due to the fact that the principle is the continuity of the contract, the return of data seems not possible; any conflicting contractual clause shall be ineffective.

In paragraph 64.j we would need clarification of the specific requirements and what the agreements should contain. Our reading of the GLs is that the contract should remind that a crisis prevention measure or a crisis management measure shall not, per se, be deemed to be an enforcement event of the contract, provided that the bills [to be defined] are paid.

Paragraph 65

Paragraph 65.a. requires to specify activities that cannot be sub-outsourced by the service provider in the contract. However, the real issue is to clearly state in the agreement with the service provider if the service provider can subcontract, and if so, which activities can be subcontracted. Therefore, this paragraph should be reworded as follows:

> "a. specify if sub-outsourcing is allowed and of which activities or any types of activities that are excluded from sub-outsourcing".

When sub-outsourcing data subject to the GDPR, the service provider must obtain prior approval from the institution (65.d) and institutions have the right to terminate the contract in case of undue sub-contracting (65.h). Even if these clauses are favourable to institutions, the "prior approval requirement" would be extremely challenging to obtain from a service provider (especially when outsourcing to a cloud service provider or to providers of other standardized services).

Paragraph 65 should be amended as follows to make clear that this risk assessment is not mandatory, but optional:

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

Moreover, if the right to terminate the agreement in case of undue sub-outsourcing is included in the contract, as required in paragraph 65.h, point g (right to oppose

subcontracting) should be optional. In any case, in the event of termination of an agreement because of undue subcontracting/increased risk, the institution should have an ample exit period to ensure orderly transfer of the service back to the institution or an alternative service provider.

In addition, there might be an inconsistency between Art 31(3) of MiFID II and paragraph 65.d. According to MIFID II, Art 31(3) "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 GLs only refer to "approval requirements" and does not specifically mention 'consent'.

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

Paragraph 66

To conclude, it seems from paragraph 66 that the sub-contractor is directly engaged with the institution. This could not be the case, as the institution negotiates only with the contractor. Therefore, the obligations list (par. 66) has to be undertaken by the provider on behalf of its subcontractor. There should also be a materiality threshold for outsourcing GLs to be applied to sub-outsourcing arrangements.

Sub-paragraph "a" should clarify if "compliance with all applicable laws" includes also laws applicable to clients of the institutions outsourcing the activity.

Paragraph 67

It is not obvious how an institution could "ensure" that the service provider appropriately oversees the sub-service providers in line with its policy. Indeed, it is possible including obligations in the agreement for the service provider to oversee sub-service providers, but it is not clear what is meant with "monitors compliance with these requirements on an ongoing basis" nor with "these requirements". Indeed, if this requirement implies continuously monitoring such oversight obligation, it could be impossible.

Furthermore, requesting that a provider acts "in line with the policy" would imply that the outsourcing institution should in a certain way impose its policy to a service provider that should have its own policy. In such situations, institutions could only incorporate certain obligations of their policy and oblige service providers to include them into their agreements with the subcontractors.

Paragraph 68

The EBA should clarify the meaning of "relevant providers": should it be considered synonymous with providers supplying "critical or important" outsourcing?

Paragraph 70

The EBA should specify if when writing "…adopt a risk-based approach to data storage and data processing location(s) and information security considerations" it refers to Risk-Based approach to locate Data Centres or based on Country-Risk.

Paragraph 72

We consider that this paragraph needs to be clarified to ensure it mainly applies to critical or important functions. Additionally, according to paragraph 93, Internal Audit function shall ensure sufficient execution of audit rights only for critical or important functions contracts.

With regards to paragraphs 72a and 72b we suggest the following amendments:

- to specify that the "complete access" includes also the possibility to have copies of relevant documents and data;
- to replace "relevant business premises ..." by "to all business premises ...relevant for providing the services";
- to specify that "unrestricted rights of inspection and auditing" includes also the possibility to have copies of relevant documents and data.

With reference to access right, it should only be required in case of outsourcing of critical or important functions.

In case of outsourcing to the cloud, given the nature of cloud services, having access to all the data centres where data is located is an unattainable requirement, since data is usually distributed and replicated among different centres. Other outsourcing services based on distributed technologies such as Distributed Ledger Technologies may raise the same difficulties regarding access and audit rights.

Therefore, it would be more effective to require Cloud Service Providers to offer mechanisms for outsourcing companies and Competent Authorities to access remotely to data, monitoring the processing of information and checking the compliance with obligations without having to get access to premises.

Moreover, we would encourage the EBA to follow the precedent it set with the Recommendations on outsourcing to cloud service providers and provide a list of clear recommendations that the entities could include in their contracts.

As we explained in Q8, having a certification from authorities at least for service providers that are highly concentrated in the financial sector would simplify and would make more efficient the audit process for financial institutions and in the end for the whole financial system.

Paragraph 73

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

Paragraph 74

We ask for the removal of the last sentence ("However they should not rely solely on those") since deciding if third-party certifications and reports are enough or not should be left to the outsourcing institution assessment. Besides, some examples or a description of which "alternative ways to provide a similar level of assurance" would be valid to comply with requirements in paragraph 79 should be given.

Paragraph 75

It is suggested to include also the reports and follow-up of Internal Audit activities performed by Internal Audit function of the service provider.

The items a-f of paragraph 75 relate to certifications as mentioned under paragraph 74 and not really to pooled audits as an institution will have influence on what is done in a pooled audit. We suggest moving these items under Section 74.

Paragraph 76

This paragraph can be interpreted so that the EBA expects each institution to secure the right to conduct its own individual penetration testing based on threat scenarios. While this is somewhat of an existing standard, a narrow view of this could be read that the institution itself can only conduct the penetration testing – this would be extremely burdensome from both an operational and a security standpoint. It would be worth clarifying that an outsourcing institution should be able to propose alternative arrangements which achieve the same outcome, e.g. through reports from reputable third-party pen testers or offering to help in the testing with the provider. This approach could be viewed as similar to the EBA's acceptance of pooled audits in paragraph 75.

Paragraph 79

In this paragraph "alternative ways to provide a similar level of assurance" are named but not specified at all. Especially the required penetration testing from paragraph 76, based on threat scenarios, would in case of a public cloud create a risk for another client's environment. Please describe alternative ways in more details.

Paragraph 81

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

Moreover, a reference in paragraph 81.b to "impediments capable to alter the performance of the outsourced service" should be better defined, as it is unclear.

The provision by which the institution is allowed to terminate the outsourcing agreement pursuant to an instruction from a competent authority will be very difficult to negotiate (paragraph 81.e). Contractual uncertainty is created by this intervention of a third party (authority). Generally speaking, the failure of a service provider to fulfil his obligations is a case of termination of the agreement.

Paragraph 82

It is our understanding that this applies mainly to critical or important functions due to proportionality aspects. Please include "for critical or important functions or where otherwise appropriate".

As a general comment, regarding the contractual phase requirements, clarification would be necessary on which requirements apply specifically to the outsourcing of critical or important functions, which to general outsourcing and which to intragroup arrangements respectively. In order to provide clarity on the specific requirements for each type of outsourcing, we would suggest having them all compiled in a specific table or diagram to identify which are applicable to each kind of outsourcing. We provide a suggestion of a table in the appendix of this document.

In addition, it would be helpful if more clarity is given on how an institution is expected to ensure compliance with the GLs during an exit caused by a shift in risk, service provider breach etc. More specifically, if there is an event that causes the institution to terminate the contract, it is likely that the institution cannot immediately and fully remedy such event but at the same time cannot immediately terminate and replace the contract either. This per definition leads to a temporary incompliance with the GLs.

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

As mentioned in the general comments above, it seems necessary to better clarify which requirements should be limited to outsourcings assessed as critical or important and not applied to other outsourcing arrangements.

Paragraph 85

The implications of paragraph 83 have to be further explained as they appear to extend the control functions currently performed by institutions. Furthermore, we ask the EBA to clarify if this paragraph requires the creation of a central monitoring body within institutions or it would be enough to ensure that this monitoring is performed by the institution's area receiving the service.

The current drafting of paragraph 85 needs to be qualified in order to clarify that the reporting escalation-process should not lead to any risk identified with regard to outsourcing arrangements being reported to the management body, but only to those deemed as material and, in any case, pursuant to the risk governance model defined by the entity. In that sense, the new proposed wording would be the following:

> *"Institutions should regularly update their risk assessment in accordance with Section 9.3 and periodically report to the management body on any* ***material*** *risks identified in respect of outsourcing of critical or important function,* ***pursuant to the risk reporting governance framework in place in each entity****."*

Moreover, a definition of "Regularly" is required.

Paragraph 88

As the term "indications" is not further defined, this could 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 it. Further the differentiation between "indications" and "recommendation/findings" (as mentioned in section 7, paragraph 45) is unclear. It raises the questions if all follow-up activities should be performed by the internal audit 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.

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

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

In general, it seems necessary to better clarify which requirements should be limited to outsourcings assessed as critical or important or to those involving extra-group providers (i.e. item 89 relating to exit strategy).

Paragraph 90

It requires that institutions are able to exit outsourcing as mentioned in the contract and its appendices, "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/important outsourcing arrangements are the only ones that can impair the financial performance, soundness and continuity of the institution. Therefore, paragraph 90 should be amended as follows to clarify that it only applies to critical outsourcing:

> "90. Institutions and payment institutions should ensure that they are able to exit critical/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:"

To this end, there should be additional guidance on the term 'sufficiently tested', to ensure there is clarity around expectations of testing the ability to shift the outsourced service to another provider or re-integrate.

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.

As a preliminary remark, from the perspective of the institutions located in those Member States where no general notification/information requirement exists (e.g. France and Germany), the introduction of a general reporting/notification/information requirement is not considered as a desirable measure. Rather, having no general notification/information requirement should be acknowledged as a best practise across the EU and these GLs should make clear that harmonisation should be undertaken in this direction. In any event, a notification requirement for intragroup outsourcing is not plausible because the main driver for the notification seems to be the need for transparency in order to identify concentration risk with providers that are not subject to supervision. Such transparency is however sufficiently given in the intragroup context. If the notification/information requirement is decided to be maintained, the following considerations apply.

The main concerns related to Section 13 are: (a) The information required to be provided to competent authorities via the "register" should be limited to item that its content is proportional and useful for supervisory purposes and split at least in two parts, one relating

to outsourcing providers (specifying if direct provider or sub-provider), the other to outsourcing contracts; (b) it is unclear whether information included in the documentation folder related to each Provider/Contract and not explicitly shown amongst the register record fields, like are represented in the "Annex I" to the Consultation paper, can be considered as available; (c) the possible impacts arising from the request to inform NCAs in a timely manner about planned outsourcing of critical or important functions are not clear. Such request does not exist in some countries (i.e. in Germany the overview to NCAs is given via regular updates). The lack of specification of the response time for NCA for assessing the information given in advance, is also considered an issue. If this timing should be too long, it could delay significantly any new outsourcing initiative or change of a provider sometimes happening on short notice). Finally, it should be clarified both the transmission channel and (in case of branches in other countries), which local NCAs (in addition to the ECB) have to be informed.

Paragraphs 93 & 94

Regarding the Notification Section, and specifically paragraphs 93 and 94, we would like to highlight the need to harmonise these procedures across the EU and with other non-financial providers.

In the Rationale & Objective part of the GLs it is stated that divergent regulatory approaches carry a risk of regulatory arbitrage which expose the EU to financial stability risks. This also applies to the notification process, for which for example each jurisdiction has developed its own notification process for cloud outsourcing. The notification process in the EU needs to be standardised across all jurisdictions.

Should the notification requirement be maintained, it should be adapted so that:

- it is thoroughly defined to avoid different interpretations by competent authorities;
- institutions are simply required to notify, *ex post*, of new outsourcing arrangements or when a function under an existing outsourcing arrangement became critical or important, but there should not be any need to wait for the response from the supervisor. Becoming an ex post requirement would avoid any competitive disadvantage between institutions subject to this requirement and those companies no required to inform any authority;
- "before they intend to enter into the new outsourcing" is replaced by "after they enter into a new outsourcing", so that there is no need to interpret in which project milestone (when choosing the provider, before signing the agreement, when going to production, when launching the pilot phase, …) has this communication to be effected and that it is possible to inform *ex post*. In line with the answer to Q6, we suggest eliminating in par. 93 any reference to cloud services that we deem are already included in the concept of critical or important function;
- intragroup outsourcing arrangements are excluded from any notification or information requirements.

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

Paragraph 103

As underlined in our answer to Q2, we deem that this paragraph should have a reference to the intragroup outsourcing which should be subject to lower compliance and reporting obligations than extra-group outsourcing agreements.

Concerning provision 103.d, further clarification would be needed regarding what is understood by "same business area". This could also become a limitation for certain areas. As an example, could Operations outsource many of its processes to multiple service providers?

Also, if competent authorities identify aggregated risks that could potentially affect financial sustainability, any action implemented should take into consideration its effects on the competitive position of the affected companies and ensure a level playing field after measures have been implemented.

Paragraph 105

The GLs as currently drafted give NCAs the discretion to limit or restrict the scope of outsourced functions or to require an exit from the arrangements. However, the GLs do not give any qualifications for what would lead to an NCA taking action on this scale nor do they explain what steps should be taken by regulators prior to this in order to ensure compliance with regulatory requirements by the regulated firm. As currently drafted, this paragraph creates substantial business case risk and could limit or handicap the use of outsourcing by regulated firms.

Any requirement to exit an outsourcing contract by an NCA should be a last resort. Prior to this step the outsourcing firm (e.g. a bank) must have substantial warning and opportunity to correct any shortcoming in its compliance and governance programme. NCAs should, as policy, have a series of 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.

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

The ratio of the template provided in Annex 1 is not clear as the consultation document does not provide with an exhaustive list of activities to be outsourced (cfr. "A different definition would require different frameworks for different activities (e.g. banking vs investment services) and leads to challenges in their application, as some arrangements affect banking, but also investment and payment services (e.g. underlying IT infrastructures)" paragraph 54). Furthermore, this list generates even more uncertainty (for example, it includes services that we consider as supplies, such as "hardware", "Use of agents"). Therefore, as already stated in our answer to Q1, we believe that providing a detailed list of exclusion would be very helpful.

Further, the various elements to be captured as a minimum in the register result to an unclear and not user-friendly template. According to text in Annex 1, we assume that the

Excel format is indeed illustrative and that banks have the mandate to develop their own register (or tool).

Q16: Are the findings and conclusion of the impact assessments appropriate and correct; where would you see additional burden, in particular in 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.)?

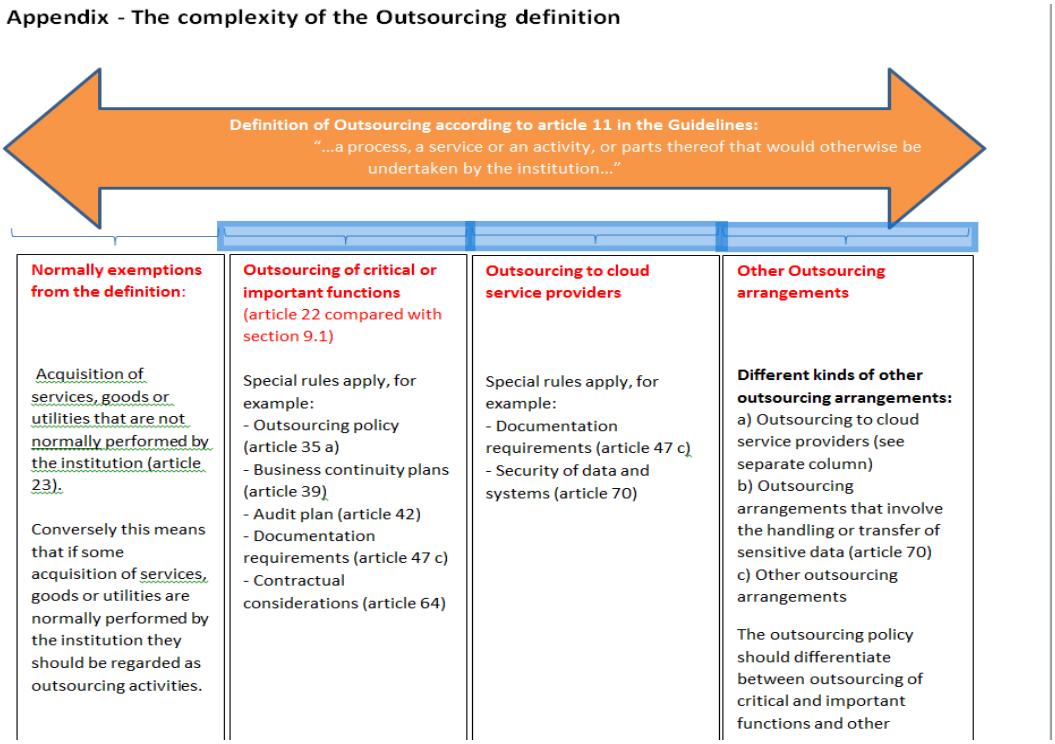
The following cases can trigger a relevant economic impact:

- The risk assessment on each single contract with third party, regardless of whether it is considered as an outsourcing contract or not (see our comments to paragraphs 24 and 57), taking into consideration the extent of the analysis (see our comments to paragraphs 59 and 61) and the frequency (our comments to paragraphs 61 and 83 "ongoing monitoring");
- The fact that outsourcing intra and extra-group are equivalent (see our comments to paragraphs 19a and 46);
- The need for assessing the risks, contractual clauses, and monitoring on a continuous basis of all sub-outsourcers as "Sub-outsourcing has been referred to in other EBA documents also as chain of outsourcing or chain-outsourcing" (our comments to paragraphs 34c ii, 47b, 56, 83 and section 10.1);
- If credit intermediaries, non-bank creditors and account information services are excluded following the assessment in section D and similar activities performed by credit, payment and e-money institutions are not excluded from the obligations in these GLs, an unlevel playing field will be created.

Moreover, the wide definition of outsourcing will create additional burdens such as financial costs, human resources, IT and administration costs. For instance, EBA's proposed definition on outsourcing is wider than the definition in place in most of the EU Member States (i.e. in the Swedish banking law and S-FSA regulation). This would affect all contract owners to review the contracts and legal resources for the negotiations. Based on previous experience, renegotiating outsourcing contracts is time-consuming and even might become not acceptable by a service provider not used to be treated as outsourcer with the linked request of specific contract clauses (i.e. audit rights). In addition, new risks such as concentration risk and step-in risk have been defined and need to be implemented in the organisation.

Appendix:

a) Complexity of the outsourcing definition:



b) A suggested summary table of requirements:

	Requirements applicable to each type of outsourcing		
	Outsourcing of critical or important functions	Outsourcing of non-critical functions	Intragroup outsourcing
Documentation	47.c	47.a 47.b	N/A
Due Diligence			
Risk assessment			
Contractual phase			
Sub-outsourcing			
Security of data and systems			
Access, information and audit rights			
Termination rights			
Oversight of outsourced functions			
Exit strategies			
Duty to adequately inform supervisors			

To be completed

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Blazej Blasikiewicz
b.blasikiewicz@ebf.eu

Iliana Koutoulakou
i.koutoulakou@ebf.eu