4 August 2017

EBF_027894

EBF RESPONSE TO EUROPEAN BANKING AUTHORITY DRAFT RECOMMENDATIONS ON OUTSOURCING TO CLOUD SERVICE PROVIDERS UNDER ARTICLE 16 OF REGULATION (EU) No 1093/2010

EBF key messages

- **EBF supports the additional guidance to the existing CEBS Guidelines.**

  We support the efforts made by the European Banking Authority (EBA) to provide additional guidance to the existing guidelines of the Committee of European Banking Supervisors (CEBS) with the aim of fostering supervisory convergence regarding the current expectations and processes for the use of outsourced cloud computing in financial services (FS). The consideration given to the proportionality principle and to the risk-based approach seems adequate to accommodate the new challenges and ensure these recommendations are future-proof. Nevertheless, it is essential that fragmentation, as regards financial supervisory regulation among Member States (MS), is avoided.

- **However, the draft recommendations remain too high-level and could leave room to multiple interpretations at national level.**

- **We are additionally concerned that the draft EBA recommendations, as they currently stand, may not be sufficient to have a positive impact on cloud adoption within financial services in Europe.**

  The draft EBA recommendations which *"aim[ed] to address the heterogeneity in the supervisory expectations regarding the technical security of cloud computing services"* (see page 6) do not seem to achieve their initial goal as they are still high-level recommendations that will not prevent different interpretations/approaches by supervisors at national level.

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

In most cases, the draft recommendations include a non-exhaustive list of general criteria, which will allow National Competent Authorities (NCAs) to include their own additional criteria or to have diverging interpretations on how to fulfil the proposed requirements. They also leave many technical security requirements to the discretion, interpretation or risk appetite of the supervisors rather than to the risk appetite of the outsourcing entity where it properly belongs. Supervisors should be able to explain the reasons (to the institution and/or the CSP) in case they do not support an initiative being outsourced to a CSP.

It is important to enable a consistent application of a risk-based approach to cloud computing in FS and to ensure that any recommendations focus on outcomes rather than listing prescriptive requirements. Competent authorities and national regulators must make every effort to comply with these recommendations without adding extra layers to the stipulated requirements.

We believe that the development of guidelines or other instruments requiring direct application by National Competent Authorities would be a better option.

The national supervisory authorities/EBA/European Central Bank (ECB) and other European institutions such as the European Commission (EC) should try to promote the safe use of cloud services in the Digital Single Market (DSM), ensuring a level playing field for all players, both within the EU and beyond. Restricting the use of cloud services will negatively affect the digital transformation of financial institutions in Europe and impede the creation of an innovative FinTech ecosystem.

The ultimate goal must be to avoid the development of different reporting criteria and/or the fragmentation of requirements between Member States.

- **EBA's objective should be to reach a point where notification on a case-by-case basis is not required at either EU or national level.**

  We have argued in the past that the requirement of notification of cloud projects on a case-by-case basis significantly increases the time to market thereby reducing the benefit of using the cloud in financial services. The industry firmly believes that EBA should aim, among others, at reaching a point where notification on a case-by-case basis is not required either at EU level or by NCAs. A first step toward this goal is to require notification only of material outsourcing, which will reduce the divergence between MS as to which different elements supervisors may take into account when evaluating cloud projects. We believe the process should allow the communication to take place once the cloud initiative is in the production phase.

- **It is important to continuously assess and update the EU outsourcing regulation to ensure it is adapted to the technology-enabled world.**

  Given the rapid growth of technology in financial services over the past few years, which is expected to continue, it is necessary to regularly assess and update the EU outsourcing regulation to make it more relevant to the technology-enabled world of finance. The most notable technologies that will benefit from cloud computing are data analytics, machine learning and distributed ledgers. In addition, many of the start-ups providing technological solutions to the banking industry or directly to consumers take a "cloud first" approach, thereby enabling greater and more efficient use of cloud computing with direct benefits on innovation and competition in financial services.

  The industry welcomes the draft EBA recommendations on using cloud computing in financial services, which represent a starting point to set up an essential baseline for a deeper contextualisation around cloud computing specificities.

However, as long as outsourcing rules designed for a different paradigm remain linked to regulatory consideration, the use of cloud in financial services will continue to suffer from unnecessary frictions. The recommendations should thus introduce further clarifications on the outsourcing concepts.

- **Cloud Service Providers should be certified based on recognised international standards.**

  Third-parties' certification mentioned in paragraph 8(b) would help financial institutions by allowing them to rely on a standard approach across Europe. We believe Cloud Service Providers (CSPs) should be certified based on recognised international standards, such as SSAE 16, SOC1 or SOC2, in order to comply with supervisors' demands in regard to risk mitigation measures. The financial services industry will work with CSPs to define how third-party audits would work and what criteria should be met so as to be accepted by EBA and NCAs. This would create a more agile process facilitating the use of CSPs in financial services.

  The adoption of base standard certifications to guarantee compliance or the definition of a cloud outsourcing banking standard against which a certification could be requested, would help outsourcing institutions and CSPs across Europe to reduce the compliance burden and increase security. A more detailed reference to a base standard certification would thus help.

- **The development of high-level principles by the industry should be favoured.**

  A non-approval of a risk analysis could come with a clear gap analysis of what control measures were lacking and would need to be implemented in order to reduce risk in any single outsourcing.

  We thus believe the creation of a harmonised European and global technology risk framework could be beneficial in alleviating or limiting many of the frictions caused by regulatory uncertainty. However, such a solution would need to be wide-ranging and led by the industry itself in order to overcome the difficulties inherent in cross-jurisdictional approaches.

  Essential benefit could be derived by EU regulators' recognition of a defined best practice.

  The EBA should work closely with the financial services industry to develop defined best practice ensuring an increased level of certainty and alleviating frictions in the current process for obtaining cloud services.

  The financial services industry will also work with CSPs to define what high-level principles should be met so as to be accepted by the EBA and NCAs. This would create a more agile process to use CSPs in financial services.

- **Further consideration should be given to the GDPR to be implemented by May 2018.**

  Cloud outsourcing includes data transfers between controllers and processors. As personal data needs to be secured at all times, adequate organisational and technical measures by both controllers and processors are vital.

  It is noted that CSPs should be considered as processors according to article 28 GDPR, meaning that CSPs shall also comply with GDPR obligations (such as article 30 paragraph 2 and articles 32 and 33 paragraph 2 GDPR).

We observe a certain overlap between local data protection laws, the future GDPR provisions for the protection of personal data and the requests made by national supervisors to perform risk analysis. We believe it is essential to take into account that data protection issues should be supervised by Data Protection Authorities (DPAs), on the basis of GDPR and local data protection laws. The National Supervisory Authorities (NSAs) should abide by the GDPR and the DPAs' decisions, if they have given permission to use a cloud service complying with all security and privacy measures. The decisions of the NSAs should not be stricter than the decisions of the DPAs as this would undermine the usage of the cloud and affect competition with other players that are not under NSA supervision.

In addition, it is important to stress that, in order to ensure a level playing field, EU members' players should comply equally with regard to GDPR, but should not be forced to comply with additional requirements to data protection, privacy and cybersecurity measures. Doing so would increase the competitive gap with non-European countries who come across fewer obstacles in using the Cloud.

- **The recommendations should explicitly mention the underlying risk driver.**

  It would also be very helpful if, for each EBA recommendation, the underlying risk driver were explicitly mentioned. This would help in understanding why a recommendation is formulated as it is.

1. Are the provisions from these recommendations clear and sufficiently detailed to be used in the context of cloud outsourcing?

In general, we believe that these draft recommendations provide additional clarifications to institutions on outsourcing to cloud service providers.

We welcome the recognition by the European Banking Authority (EBA) of the existing significant levels of uncertainty regarding the supervisory expectations that apply to outsourcing to Cloud Service Providers (CSPs) (mainly due to differences in the national regulatory and supervisory frameworks for cloud outsourcing) and the resulting barrier to institutions using cloud services.

We support the efforts made by the EBA to provide additional guidance to the existing guidelines of the Committee of European Banking Supervisors (CEBS) with the aim to foster supervisory convergence regarding the current expectations and processes for the cloud. The consideration given to the proportionality principle and the risk-based approach seems adequate to accommodate the new challenges and ensure these recommendations are future-proof.

This said, although the recommendations represent a positive first step to bringing harmonisation and avoiding national regulatory and supervisory differences, the development of guidelines or other instruments requiring direct application would be a better option than recommendations which do not prevent different approaches/ interpretations by supervisors at national level. In most cases, the recommendations include a non-exhaustive list of general criteria, which will allow National Competent Authorities (NCAs) to include their own additional criteria or to apply diverging interpretations on how to fulfill the proposed requirements.

In our view, the list of criteria should not leave room for interpretation. It is important to enable the consistent implementation of a risk-based approach and that this implementation is built on principles and outcomes rather than on a prescriptive list. Competent authorities and financial institutions must make every effort to comply with these recommendations. It is indeed important that the local regulators do not add extra layers to those requirements.

The EBA should work closely with the financial services industry to develop defined best practices. Such best practices will provide the industry with the level of certainty it requires and will alleviate frictions in the current process for obtaining cloud services without requiring that EBA sets out more prescriptive regulation, which in turn would make the recommendations difficult to adapt to future needs. The financial services industry will also work with CSPs to define what high-level principles should be met so as to be accepted by the EBA and NCAs. This would create a more agile process to use CSPs in financial services.

In addition to the above general comments, please find below our detailed opinion on some of the observations.

CHAPTER 2 – SUBJECT MATTER, SCOPE AND DEFINITIONS

DEFINITIONS

As a general comment, we observe that the definition of cloud computing mentioned in the draft recommendations corresponds to the definition of the National Institute of Standards and Technology (NIST) Special Publication SP 800-145, published in September 2011.The definition provided by the draft EBA recommendations remain however more concise, which may lead to confusion. We therefore recommend to make direct reference to the NIST SP 800-145, which provides a complete definition, as well as to the ISO-IEC 17788-2014, which also represents an international standard which is technology- neutral.

In view of the above, we would request to remove all the definitions mentioned in the summary table at the bottom of page 10. A second reason for the request to remove this table would be that the definition of the NIST SP 800-145 distinguishes between IaaS, PaaS and SaaS, while the draft EBA recommendations seem to apply to any and all forms of cloud computing.

CHAPTER 4 – RECOMMENDATIONS ON OUTSOURCING TO CLOUD SERVICE PROVIDERS

CHAPTER 4.1 - MATERIALITY ASSESSMENT

Suggestion for amendment :

1. Outsourcing institutions should, prior to any outsourcing of their activities, assess which activities should be considered as material ***in line with the list of activities subject to mutual recognition mentioned in annex 1 Directive 2013/36/EU[1].*** *Institutions should perform this assessment of the activities' materiality on the basis of CEBS guidelines and, in particular as regards outsourcing to cloud service providers, taking into account all of the following:*

(a) the criticality and inherent risk profile of activities to be outsourced i.e. activities that are critical to the business continuity/viability of the institution and its obligations to customers,

~~***(b) the direct operational impact of outages, and related legal and reputational risks,***~~

~~***(c) the impact any disruption of the activity might have on their revenue prospects,***~~

~~***(d)***~~ ***(b)*** *the potential impact that a confidentiality breach or failure of data integrity could have on the institution and its customers,*

(c) in cases where the activity is identical or very similar, the outsourcing institutions should be able to rely on previous similar assessments to avoid unnecessary double assessments and take into account the information already communicated.

1. Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance

- We welcome the clarification of the required materiality assessment for cloud computing. We agree with the risk-based approach adopted in the guidelines as such an approach remains, in our view, the best way to ensure appropriate risk control and mitigation. In addition to a risk-based approach, the principle of proportionality is important to consider.

  There may be instances where the use of cloud computing could be considered by regulators/supervisors as resulting in certain risks (e.g. exit concerns), but - to the contrary - the use of the cloud could contribute to significantly reduce risks compared to the on-premise present situation. **Cloud offers a lot of opportunity to materially increase security and facilitate compliance with GDPR**.

- We would like to stress that materiality assessment differs from the requirements of other risk assessments. Despite the definition of materiality which is provided and based on the CEBS Guidelines, **the definition provided by the draft EBA recommendations is not sufficient as it does not give any qualitative or quantitative criteria to objectively establish if a service is considered material or not.** The industry should therefore participate to the elaboration of criteria which will be recognised by the National Competent Authorities (NCAs) in order to ensure legal certainty, achieve a certain harmonisation and manage cloud outsourcing of activities with low risk impact.

  As a suggestion for amendment, we believe that the term "material" should be limited to the core business by reference to annex 1 Directive 2013/36/EU *"List of activities subject to mutual recognition".*

  The following wording is therefore proposed:

  "1. Outsourcing institutions should, prior to any outsourcing of their activities, assess which activities should be considered as material ***in line with the list of activities subject to mutual recognition mentioned in annex 1 Directive 2013/36/EU*** [(1)]. *Institutions should perform this assessment of the activities' materiality on the basis of CEBS guidelines and, in particular as regards outsourcing to cloud service providers, taking into account all of the following:"*

  (1) Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance

- **The EBA recommendations should also indicate the possibility of avoiding double assessment in cases the activity is identical or very similar.**
  - It should be indeed possible to rely on initial assessments conducted for identical or similar activities.
  - In case new aspects should be taken into account for the assessment, this assessment should only cover the points which are diverging from the previous one. Minor changes should not justify a completely new assessment. There could also be cases where the assessment is not necessary: for example when adding an activity into a framed contract with the same or similar objective, only concise additional information might be required, meaning that a new assessment should not be required.
  - If nevertheless an assessment is needed, a quick review should be conducted within a shorter period than the one usually conducted for a complete assessment.
  - It is important that the EBA recommendations also cover cases where a service added into a contract has already been communicated or accepted by the authority, and clarify what should (or shouldn't) be communicated/notified to the authority.

The following wording is therefore proposed:

"(c) in cases where the activity is identical or very similar, the outsourcing institutions should be able to rely on previous similar assessments to avoid unnecessary double assessments and take into account the information already communicated."

- ***"(b) the direct operational impact of outages, and related legal and reputational risks"***

  We propose to delete these criteria as it is incorrectly assuming that the risk of disruption increases with a CSP. The opposite may well be the case, depending upon the size of the bank vs the CSP.

- ***"(c) the impact any disruption of the activity might have on their revenue prospects"***

  We propose to delete this sentence since this cannot be allocated to a single outsourcing. Other methods are generally in place to analyse this aspect.

- **Among the four criteria mentioned, only criteria (a) and (d) should be maintained**

  It is important that all banks make the necessary assessments and report them to their NCA. This should in turn ensure that all institutions and NCAs, on aggregate, take systemic risks into consideration. We consider however that among the four criteria mentioned, only criteria (a) and (d) should be maintained. "(a)" is specific to cloud outsourcing and "(d)" covers GDPR considerations. The rest of the criteria are not specific to outsourcing, meaning that they must be taken into account and be assessed in any service, even for those offered directly without any outsourcing agreement.

CHAPTER 4.2 – DUTY TO ADEQUATELY INFORM SUPERVISORS

- The current draft recommendations require significant amounts of duplication in form and content of the information to be collected and reported to regulators/supervisors. For example, regarding personal data outsourced that implies an international data transfer outside the EU, it would mean reporting/communicating information to Data Protection Authority (DPA) and to the national supervisory authorities which might have different approaches. As other examples, paragraph 4.2.2 lists the information to be made available for material outsourcing, paragraph 4.2.3 lays out additional information on the firm's risk analysis that may be requested, and paragraphs 4.2.4 and 4.2.5 detail the requirements of a register of outsourced activity including non-material activity which is to be maintained at institution and group level and submitted to NCAs upon request.
- The level of duplication is increased by the right of NCAs to request additional information in all cases as per paragraph 3. We thus question how this information will be understood by NCAs and whether such an *ad hoc* collection of information would create a potential for continued variation in the regulatory approach across national jurisdictions, which would go against the purpose of these recommendations. We would therefore advocate for a common risk-based approach across national jurisdictions.

PARAGRAPH 2

Suggestion for amendment :

2. Outsourcing institutions should adequately inform the competent authorities of material activities being outsourced to cloud service providers. Institutions should perform this ***~~on the basis of~~ as required by*** *paragraph 4.3. of the CEBS guidelines and, in any case, make available to the competent authorities the following:*

(a) name of the cloud service provider, name of the parent company (if any);

(b) description of the activities and data outsourced;

~~(c) country where the service is performed (including location of data);~~

***~~(d)~~ (c)** service commencement date;*

***~~(e)~~ (d)** last contract renewal date (where applicable);*

***~~(f)~~ (e)** the applicable law governing the contract;*

***~~(g)~~ (f)** service expiry or next contract renewal date.*

- In our view, **this recommendation neither establishes precisely what has to be communicated, nor the Authority/Authorities (national and/or European Central Bank level) to be informed nor the procedure and deadline for Authorities to accept/not oppose the outsourcing of the service**.

  Currently, some jurisdictions do not observe any authorisation/approval procedure but rather provide "administrative silence" or "silent assent" after one month. Moreover, even if there are security checks conducted by the supervisor, banks never know in advance what would be required to comply with those requirements.

- **One of the main issues is to make a distinction between non-material and material activities**. We believe that non-material services should not be subject to any notifications in line with the CEBS guidelines 5 (2006) which clearly state that "*there should be no restrictions on the outsourcing of non-material activities*" and "*in such cases the outsourcing institution does not need to adequately inform its supervisory authority".* For non-material services there are several items which may not be available for the assessment of the service that an institution wants to outsource. In particular, if an outsourcing institutions' initial assessment reveals that the service to be outsourced to the cloud is in no way material, several requirements including the execution of a fully documented in-depth risk analysis, privacy assessment and legal/contractual screening are replaced by a different assessment requiring less documentation. **Therefore, <u>for non-material cloud services</u>, we would prefer deleting the proposed EBA requirements for recording information under requirements 5(a) concerning 2(c), 2(e), 2(f), 2(g) and the recommendations under 5(e) and 5(f) (see also our comments to paragraph 5).**
- **We believe that the communication of contractual agreements with CSPs once signed, and the security policy and criteria agreed by the outsourcing institution and the CSP should be enough. Once the NCA has reviewed and validated the underlying conditions and obligations, it should not be necessary to notify the provision of any service within this already assessed framework.**

- Finally, as mentioned above, there remains room for uncertainty and variation among jurisdictions following the recommendations in the EBA consultation. **The EBA and NCAs should thus consider accepting industry best practice for the reporting of outsourced activities.** The industry would benefit from standardisation in reporting requirements which could be achieved through industry best practice. Regulators would benefit from a more comprehensive and less *ad hoc* approach to information collection.

- ***"(c) country where the service is performed (including location of data)",***

  It is not clear what *'including location of data'* means, or what level of detail is required here. Overall, this heavy focus on data locality is seen as problematic, especially given that, currently and even more in the future, it is expected that technology will continue to evolve in a direction where physical location of data will become less and less clear. These recommendations should focus on ensuring access to data from the location of the outsourcing institution and not on the location of data that is already regulated by applicable data protection regulations.

  It is also important to stress that according to our interpretation of the CEBS guidelines paragraph 4.3 does not stipulate that the location of data, via reporting of the country where the service is performed, is required.

  For those reasons, we propose that requirement "(c)" is removed and in the first sentence of paragraph 2 *"on the basis of" is replaced by "as required" [by paragraph 4.3].*

PARAGRAPH 3

Suggestion for amendment:

3. Further to the information provided, ***if the information already provided is not sufficient,*** *in accordance with the previous paragraph, the competent authority may ask the outsourcing institution:* ~~***for additional information, on its risk analysis for the material activities outsourced, such as***~~

(a) to be informed *whether the cloud service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution;* ***However, it is not necessary for the national competent authority to see or approve the cloud service provider's business continuity plan;***

(b) whether the outsourcing institution has an exit strategy in case of a termination by either party or disruption of provision of the services by the cloud service provider;

(c) ~~***whether the outsourcing institution keeps the skills and resources necessary to adequately monitor the outsourced activities.***~~ ***whether the cloud provider adopts a market standard risk management framework and internal control system, and supplies periodically the outsourcing institution with the relevant information.***

- In our views the sentence *"in accordance with the previous paragraph, the competent authority, may ask the outsourcing institution for additional information, on its risk analysis for the material activities outsourced"* leaves a certain flexibility to the national supervisors to ask or not additional information, which could lead to a lack of harmonisation among supervisors as each local supervisor may ask for different extra information. We believe it could slow down or even block the use of cloud services due to a continuous requirement for extra information.

  We therefore believe that the information requested should be limited and requested only when the information already provided is not sufficient.

  The wording *"if the information already provided is not sufficient"* should be therefore added and *"for additional information, on its risk analysis for the material activities outsourced, such as"* should be deleted in the first sentence of paragraph 3.

  The following wording is therefore proposed:

  "3. Further to the information provided, ***if the information already provided is not sufficient,*** *in accordance with the previous paragraph, the competent authority may ask the outsourcing institution:"*

- In addition, further clarification is needed regarding the following points:

  - ***"(a) whether the cloud service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution;"***

    It is not clear whether it would be enough to merely know that the CSP has a business continuity plan or if the plan would need to be provided to the outsourcing institution and/or the supervisory authorities. If the latter is required, this may create significant difficulties for the conclusion of a contractual agreement between a financial/outsourcing institution and a CSP, due to the diverging interpretations of NCAs of what constitutes a sufficient business continuity plan (requirements the financial institutions will have to comply with).

    Therefore, we recommend that the EBA amends paragraph 3(a) by adding *"to be informed"* at the beginning of the paragraph and add the following sentence *"However, it is not necessary for the national competent authority to see or approve the cloud service provider's business continuity plan"*

    In addition, the "(a)" requirement becomes redundant, if CSPs can show they are complying with certain standards or regulations such as the Data Protection requirements, NIS Directive, etc. If supervisors are already aware that certain CSPs are homologated with this requirement, outsourcing institutions should not need to submit evidence of such information each time they need to work with a specific homologated CSP.

    The financial industry will also work with CSPs to define what criteria should be met so as to be accepted by the EBA and NCAs.

    The following wording is therefore proposed:

    "(a) to be informed *whether the cloud service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution;* ***However, it is not necessary for the national competent authority to see or approve the cloud service provider's business continuity plan;"***

- ***"(c) whether the outsourcing institution keeps the skills and resources necessary to adequately monitor the outsourced activities."***

  It is not clear how to provide evidence that the required skills are present. In addition, this requirement does not seem to take into account that certain outsourced activities maybe automatised and do not need human resources (and therefore skills), which is actually one of the main advantages of certain cloud services.

  We therefore consider that the initial sentence should be deleted and replaced by the following one:

  "(c) whether the cloud provider adopts a market standard risk management framework and internal control system, and supplies periodically the outsourcing institution with the relevant information"

PARAGRAPH 4

Suggestion for amendment:

4. The outsourcing institution should maintain an updated register with information related to all its material ***~~and non-material~~*** *outsourced activities at institution and,* ***if required by the National Competent Authority, at*** *group level.* ***This register should include only the core elements related to an individual outsourcing file.*** *The outsourcing institution should make available to the competent authority, upon its request, a copy of the outsourcing agreement and related information recorded in that register* ***~~irrespective of whether or not the outsourced activity had been assessed by the institution as material~~****.*

- We agree that the outsourcing process should be fully documented, and under management control. Nevertheless, the approach concerning the maintenance of an updated register with information related to material outsourced activities (on group level, level of every legal entity, senior management level) should be left at the discretion of the outsourcing institution, in alignment with the principle of proportionality.

  Some banks involve a number of largely independently operating institutions active inside and outside of the European Monetary Union (EMU). Almost all processes are set up in a local context, and maintaining an outsourcing register at group level on a permanent basis is therefore problematic as these institutions lack supporting management structures or information systems to collect and process this information.

  The paragraph should therefore be amended by adding the following wording *"if required by the National Competent Authority, at"* before the wording *"group level"*, to provide a certain flexibility and reflect the practice that most of the banks are only prepared to provide information at institution level.

- In alignment with the principle of proportionality, an approach explicitly confirmed by the EBA in the draft recommendation, we would recommend limiting the register under recommendations 4 and 5 to material cloud services only, the same way as for 4.2.2.

  Registrations should therefore be limited to:

  - Material activities (excluding non-material files);
  - Only the core elements related to an individual outsourcing file (name of the service provider, short description of the activities concerned, renewal or expiry date, date and management body that assessed the materiality).

Because the requirement *"(…) The outsourcing institution should make available to the competent authority, upon its request, a copy of the outsourcing agreement and related information (…)"* is only necessary for material outsourcings and thus not necessary for non-material outsourcing, the following provision should be deleted *"(…) irrespective of whether or not the outsourced activity had been assessed by the institution as material."*

- We would also welcome some clarifications on whether this new register is to be created exclusively for the purpose of outsourcing cloud services. The EBA should clarify that the register will only refer to new contracts. Existing outsourcing services will not be concerned until the contract is renewed.
- In the EBF view, a risk-based approach to what is included in the register should be favoured. Best practices could also help set these guidelines.

The following wording is therefore proposed:

"4. The outsourcing institution should maintain an updated register with information related to all its material outsourced activities at institution and, ***if required by the National Competent Authority, at*** *group level.* ***This register should include only the core elements related to an individual outsourcing file.*** *The outsourcing institution should make available to the competent authority, upon its request, a copy of the outsourcing agreement and related information recorded in that register"*

PARAGRAPH 5

Suggestion for amendment :

5. In the register referred to in the previous paragraph, ***for cloud service providers****, the following information should* ~~***at least***~~ *be included* ***and is likely to be sufficient****:*

(a) those information referred to in paragraph 2 (a) to ~~***g***~~ ***(f) for material outsourcing*** *and in paragraph 2* ***(a) to (c) for non-material outsourcing****, if not yet provided ;*

~~***(b) type of outsourcing (IaaS, PaaS, SaaS, public/private/hybrid/community);***~~

~~***(c)***~~ ***(b)*** ~~***parties***~~ ***the outsourcing institutions*** *receiving cloud services under the outsourcing agreement;*

~~***(d)***~~ ***(c)*** *approval for outsourcing by the management body or the committee designated by* ~~***it***~~ ***the appropriate responsible party,***

~~***(e) name of the main subcontractor if applicable;***~~

~~***(f) country where the cloud service provider / main subcontractor is registered;***~~

~~***(g)***~~ ***(d)*** *whether the outsourcing has been assessed as material (yes /no);*

~~***(h) date of institution's last materiality assessment of the outsourced activities;***~~

~~***(i)***~~ ***(e)*** *cloud service provider /* ~~***significant***~~ ***essential*** *subcontractor supports business operations that are* ~~***time***~~ *critical (yes/ no);*

~~***(j)***~~ ***(f)*** *assessment of the* ***cloud service provider–activity****'s substitutability as* ~~***easy, difficult or impossible***~~ ***short, medium and long****;*

~~***(k)***~~ ***(g)*** *identification of an alternate service provider, where possible;*

~~(l) date of the last due diligence~~ (h) Whether a due diligence on the outsourcing or subcontracting arrangement has been performed.

As a general comment, we observe that risk management duties by CSPs are not mentioned in the document. Because national competent authorities already request an *'outsourcing register'* for all outsourcing contracts, the required information for outsourcing to CSPs should be duly integrated. Taking into account that not all national competent authorities have defined a standard dataset to be included in the register and some of the information required and requested by national regulations only concerns material outsourcing, we suggest amending the first part of 4.2 paragraph 5 by referring to *"for cloud service providers",* deleting *"at least"* and including *"and is likely to be sufficient"*.

The amendment proposed should be taken into account because as currently drafted this sentence encourages "gold plating" thereby challenging the goal of harmonisation which is one of the purposes of these recommendations. While we acknowledge that the EBA is trying to create a minimum rather than a maximum list of information, the removal of the phrase *'at least'* and the addition of *'and is likely to be sufficient'* would limit creating expectations that NCAs should request additional information about material activities, without removing their ability to do so, if necessary.

The following wording is therefore proposed:

"5. In the register referred to in the previous paragraph, ***for cloud service providers****, the following information should be included* ***and is likely to be sufficient****:*

(a) those information referred to in paragraph 2 (a) to ***(f) for material outsourcing*** *and in paragraph 2* ***(a) to (c) for non-material outsourcing****, if not yet provided;"*

In addition, further clarifications should be provided on the following provisions:

- ***(b) type of outsourcing (IaaS, PaaS, SaaS, public/ private/ hybrid/ community);***

  We believe (b) requirement should be removed.

  The definitions of the various outsourcing services and deployment models continue to evolve following the development of new technologies. Consequently, using such a classification would create several difficulties including a risk of the recommendations becoming quickly outdated, which in turn would necessitate a constant and burdensome review and update by the EBA and the national competent authorities.

  Indeed, almost a limitless number of variations in service models already exist meaning that many experts rely on XaaS as a category to represent the new and as-of-yet unclassified types of cloud services. Likewise, the deployment models can often be a combination of on- and off-premise technologies, themselves open to definitional debates.

  Finally, it is important to clarify that, if the main objective of the identification of the type of cloud service and of deployment model is to assess the risk involved in any outsourcing activity, the type of outsourcing is not an efficient proxy to be used. We recommend that the risk assessment performed by the outsourcing institution is used instead.

- ***(c) parties receiving cloud services under the outsourcing agreement;***

  It is not clear who could be the 'parties' receiving the cloud services. Clients of the bank? The bank itself? In our view, 'parties' should refer to the outsourcing institution receiving cloud services within the specific outsourcing agreement. We therefore suggest replacing *'parties'* by *'the outsourcing institutions'.*

  The following wording is therefore proposed (new (b) replacing (c)):

  *"**(b) the outsourcing institutions** receiving cloud services under the outsourcing agreement;"*

- ***(d) approval for outsourcing by the management body or the committee designated by it;***

  We understand that the EBA decided to refer to "*or the committee designated by it"* as it is conscious that it is not necessarily the management body which provides the approval for the outsourcing.

  We suggest simply referring to the entity/function (management body, specific committee etc.) entitled to give the authorisation for the outsourcing activity, since it is not necessarily the management body or a committee. As an alternative, we believe that it is important to refer to "*the appropriate responsible party".*

  The following wording is therefore proposed (new (c) replacing (d)):

  *"**(c)** approval for outsourcing by the management body or the committee designated **by the appropriate responsible party**",*

- ***(e) name of the main subcontractor if applicable;***

  - As a general comment, we believe that an outsourcing institution should retain the ability to monitor and control its outsourcing services when a CSP uses a subcontractor. So an outsourcing agreement should necessarily include the rules and limitations governing the relations between the outsourcing institution, the CSP and its subcontractor. This means that the CSP should be contractually liable for the performance and risk management practices of its subcontractor and for the subcontractor's compliance with the provisions mentioned in the contractual agreement with the service provider.
    The sub-contracting of any part of the outsourced material activities should also be subject to the outsourcing institution's prior approval. It is important to take into account that there can be more than one subcontractors/cloud service providers involved in one process.
  - Considering those elements, it is not clear what *"main subcontractor"* stands for. The CSP? The main subcontractor of the CSP?

    We understand that this sentence might want to capture smaller CSPs using other major cloud services (e.g. a cloud service listed in a Cloud Service Provider Market Place running entirely on this CSP). This sentence however is problematic if it directly involves these major CSPs which use hundreds of subcontractors and often none of them pose a significant risk since they do not touch core functions.

    We therefore suggest deleting provision (e).

- ***(f) country where the cloud service provider / main subcontractor is registered;***

  As already mentioned above, for non-material services there are several items which may not be available using the current risk-based approach of evaluating new cloud services. In particular, if an initial assessment reveals that a cloud service is in no way material to certain banks, several requirements including the execution of a fully documented in-depth risk analysis, privacy assessment and legal/contractual screening are replaced by a more lightweight assessment that entails less documentation. Therefore, for non-material cloud services, we would prefer to waive the proposed EBA requirement for recording information under recommendation 2(c), 2(e), 2(f), 2(g) and under recommendation 5(e) and 5(f).

  We therefore suggest the deletion of 5(f)

- ***(h) date of institution's last materiality assessment of the outsourced activities;***

  We suggest the deletion of provision (h) because it means that the materiality assessment has to be verified periodically.

- ***(i) cloud service provider / significant subcontractor supports business operations that are time critical (yes/ no);***

  The reference to '*significant*' should be better explained or replaced by '*essential*', while also the definition of what is '*time critical*'. We would therefore suggest deleting the word '*time*' in order to avoid any legal uncertainties and be fully accurate.

  The following wording is therefore proposed (new (e) replacing (i)):

  *"**(e)** cloud service provider / **essential** subcontractor supports business operations that are critical (yes/ no);"*

- ***(j) assessment of the cloud service provider's substitutability as easy, difficult or impossible;***

  - We believe this requirement creates duplication with requirements under exit strategy. Moving a service from one CSP to another will be accounted for in the contract agreed between the outsourcing /financial institution and the CSP. Thus, it is more appropriate to refer to it only in the contingency and exit strategy (rather than in the part concerning the register).
  - Furthermore, it is important to stress that *'substitutability'* does not refer to the CSP, but the activity itself. The phrasing of the recommendations should be changed to reflect this.
  - Finally, the use of the terms *'easy, difficult, impossible'*, could generate uncertainties among both outsourcing/financial institutions and CSPs. These should be removed in favour of a time-based classification of *'short, medium and long'*, which could still be general and lack "definitional" certainty, but are easier for the outsourcing/financial institution to rank and quantify. Further certainty could be provided by industry best practices regarding time-based requirements.

  The following wording is therefore proposed (new (f) replacing (j)):

  "***(f)** assessment of the **cloud service provider activity**'s substitutability as **short, medium and long**;*

- ***(l) date of the last due diligence on the outsourcing or subcontracting arrangement.***

  We understand that banks have to run a due diligence process to check whether CSP outsourcing arrangements are suitable. This requirement should be based on a self-assessment by the cloud service provider. Nevertheless, it would be helpful to clarify further the reference made to '*Due diligence*'.

  'Due diligence' should involve an evaluation of all relevant information about the service provider. At least the following information in relation to CSP should be provided:

  - Financial strength and resources
  - Corporate governance and business reputation
  - Risk management framework and capabilities
  - Experience and ability to implement and support the outsourcing contract
  - Security, internal controls and audit coverage
  - Business Continuity & Disaster Recovery Capabilities
  - Insurance coverage
  - Ability to comply with laws and regulations
  - Reliance on and success in dealing with subcontractors

  We therefore believe that the wording *"date of the last due diligence on the outsourcing or subcontracting arrangement"* should be replaced *by "Whether a due diligence on the outsourcing or subcontracting arrangement has been performed".*

  The following wording is therefore proposed (new (h) replacing (l)):

  "(h) Whether a due diligence on the outsourcing or subcontracting arrangement has been performed."

CHAPTER 4.3 – ACCESS AND AUDIT RIGHTS

NEW OPTION TO BE CONSIDERED: AUDIT PERFORMED BY AN INDEPENDENT THIRD PARTY ACCEPTED BY SUPERVISORY AUTHORITIES

The issue related to the complexity of auditing services outsourced to the cloud has long been known. Banks are required to cooperate with regulators, and generally ensure (on-site) access rights to records, premises and personnel. However, physical access to premises hosting the cloud infrastructure is often a point of tension in negotiations with CSPs, who may be reluctant to allow customers into their data centres for legitimate security and confidentiality reasons. Furthermore, in a globalised and distributed cloud model, access to the physical location delivers a negligible outcome, other than the most basic one of physical security and access checks. In contrast, a virtual audit of data can be of much greater relevance to ensuring appropriate controls are in place.

Complex supply chains such as a Software as a Service (SaaS) solution built on another provider's infrastructure/platform also make securing rights to have access / to interview personnel (for each party of the supply chain) challenging in negotiations.

Effective identification, monitoring and reporting of risk is thus more challenging in many cloud environments given the lack of visibility over the whole supply chain of the technology stack.

This challenge is further driven by an ambiguity concerning how far auditing rights should be exercised throughout the supply chain.

Without clarity concerning what is required to comply with regulatory requirements, banks may either look to secure rights extensively all the way down the supply chain, or may be forced to take on additional risk in not ensuring sufficiently extensive audit rights.
The challenge for CSPs is compounded by the large number of customers and by the standardised offering which leads to a high level of complexity when giving individual customers the right to audit.

Besides the CSPs' operational responsibility regarding service provisioning, banks as data controllers are liable for the data stored and processed. As such, cloud service consumers need assurance that all contract terms are fulfilled. However, some CSPs are not always able to comply with specific contract terms, such as the right to audit. Hence, a common approach should be developed so as to facilitate compliance with a commonly understood set of minimum requirements to operate in Europe.

Formal assurance should be achieved through individual audit agreements. Ensuring harmonised sets of certifiable controls for auditing should be the main aim.

The work conducted in 2015 by ENISA together with the Cloud Select Industry Group on Certification Schemes and the European Commission regarding the "Cloud Certification Schemes Metaframework (CCSM)" should be welcomed as well as the standards promoted by the NIS Directive. The CCSM maps out detailed security requirements used in the public sector to describe security objectives in existing cloud certification schemes. However, a step further should be undertaken to coordinate the development of sets of certifiable controls (interesting in this regard is the work carried out by the Cloud Security Alliance as part of the STAR certification and the SSAE 16 type II, which is an internationally recognised standard to audit on security and governance as well as the CSA's Guidance and Cloud Controls Matrix which maps CSA recommendations against other control frameworks including ISO 27001/2, BITS v5/6 and ENISA IAF.)

We would therefore strongly invite the EBA to consider the following option:

In our view, **the audit should be performed by an independent third party, and should be accepted by supervisory authorities as a guarantee of regulatory compliance and real implementation of the recognised measures and controls. Thus, banks subscribing to the audited cloud service, would be able to rely on these audit results without having to carry out their own audit of the CSP's controls.**

Nonetheless, this must not preclude banks from keeping their contractual audit rights, to be activated on a case-by-case assessment of the risks. Indeed, banks need to assess, depending on the result of the due diligence, whether they need an external audit by an independent third party or whether they can audit directly.

Also, a harmonised approach to defining the level of access to the business premises of the CSP that need to be contractually ensured by banks, should be taken by European Supervisory Authorities and National Financial Supervisory Authorities and be clearly communicated in order for the CSPs to be able to adapt their offering to the banking sector in accordance with such requirements.

FOR INSTITUTIONS:

PARAGRAPH 6:

- ***"(a) to provide the institution, to any third party appointed for that purpose by the institution and the institution's statutory auditors full access to its business premises, … (right of access);"***

Suggestion for amendment :

a) to provide to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor ***~~full~~ access rights*** *to its business premises,* ***with the purpose of inspecting the data centre facilities for physical and environmental controls and the possibility to provide evidence in an electronic/automated way, if possible.~~ including the full range of devices, systems, networks and data used for providing the services outsourced (right of access)~~****;***

Business premises may include head offices, operations centres which are relevant for the exercise of effective oversight, but does not necessarily include data centres or access to all business premises. For example, service providers may, for legitimate security reasons, limit access to some sites – such as data centres.

- As a general comment, we believe that the current requirement could give the outsourcing institution access to any part of the CSP's premises and resources irrespective of the connection to the outsourcing institution in question. That could create a risk (e.g. risk related to security operation, confidentiality or intellectual property) for the CSP and a substantial contractual hurdle.

  Past experience indicates that major CSPs are not willing to provide such extensive access and audit rights in their contracts. What is more, from a bank's risk management perspective, we do not see this as beneficial. With regards to right of access, the added value of physical facility access is extremely low in modern-day technology environments where data is physically and geographically dispersed across many systems, data centres and even countries. One effect of this requirement is the need for extremely extended contractual negotiations between financial institutions and CSPs, resulting in an extended time to market for the cloud service and even situations where banks are prevented from using the cloud service at all. In summary, the negative impact of this requirement can be very high compared to its potential benefit, considering that it could even make cloud usage impossible.

  In addition, we believe the EBA should be more specific on the objective of this recommendation as currently it suggests that via third party the supervisor wants to obtain full access to business premises. If the objective is to know where the data is located and ensure that the data is geolocalised in the datacentre, then the option to obtain the evidence in an electronic /automated way, without human intervention, should be considered.

  We therefore recommend this to be reformulated so that the wording can be used in a contract.

  This measure should be amended to describe what kind of access is needed and whether other methods could be used (electronic/automated methods). If the access right is kept, it should be restricted to access to the resources used to directly deliver the service and **limited to data centre visits only, with the purpose of auditing physical & environmental controls (see also next section below on right of audit).**

The following wording is therefore proposed:

"(a) to provide to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor ***access rights*** *to its business premises,* ***with the purpose of inspecting the data centre facilities for physical and environmental controls and the possibility to provide evidence in an electronic/automated way, if possible.***

Business premises may include head offices, operations centres which are relevant for the exercise of effective oversight, but does not necessarily include data centres or access to all business premises. For example, service providers may, for legitimate security reasons, limit access to some sites – such as data centres."

- ***"(b) to confer to the institution, to any third party appointed for that purpose by the institution and the institution's statutory auditor unrestricted rights of inspection and auditing (right of audit)."***

Suggestion for amendment:

(b) *to confer to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor* ***either direct or indirect, yet principally*** *unrestricted rights of inspection and auditing (right of audit).*

From a banking perspective, we agree that the right of audit must be ensured. This principle receives strong support but, as mentioned above, there is also concern that the draft recommendation's wording may lead to extended contractual negotiations and ultimately even obstruct certain cloud service usage due to the unwillingness or inability of some CSPs to comply with the measure. Currently this is one of the main frictions in the use of cloud services in finance faced by the majority of banks and is a major underlying reason why the adoption of cloud in financial services is so much slower in comparison to non-regulated industries.

We suggest the paragraph to be rephrased so that the outsourcing institution is required to include contractual safeguard which will ensure it does not lose its ability to execute independent audits. It should be done in a way that does not restrict the bank's ability to manage risks and keep oversight while also being manageable for a CSP.

The following wording is therefore proposed:

"(b) to confer to the institution, to any third party appointed for that purpose by the institution and to the institution's statutory auditor ***either direct or indirect, yet principally*** *unrestricted rights of inspection and auditing (right of audit)."*

PARAGRAPH 7

Suggestion for amendment:

7. The effective exercise of the rights of access and audit should not be impeded or limited by contractual arrangements. When the performance of audits or the use of certain audit techniques might create a risk for another client's environment ***or the service provider's own business,*** *alternative ways to provide a similar level of assurance required by the institution should be agreed upon.*

The protection should not only apply to the outsourcing institution but also to the cloud service provider's own business from undue risk. We therefore suggest adding *"or the service provider's own business"*.

It is also unclear what *'alternative ways'* stands for, as well as the examples mentioned.

The following wording is therefore proposed:

"7. The effective exercise of the rights of access and audit should not be impeded or limited by contractual arrangements. When the performance of audits or the use of certain audit techniques might create a risk for another client's environment ***or the service provider's own business,*** *alternative ways to provide a similar level of assurance required by the institution should be agreed upon."*

PARAGRAPH 8

Suggestion for amendment:

8. The outsourcing institution should exercise its right to audit and its right to access in a risk-based manner. Where an outsourcing institution does not employ its own audit resources ***or where to do so would be impractical,*** *it should at least consider to use one of the following tools:"*

(a) ***Execution of a third-party (~~P~~p****ooled****) audit****s that is either executed by one of the participating outsourcing institutions or a trusted third-party, where the participating outsourcing institutions have the freedom to participate in determining the audit scope & where the audit is also paid by the outsourcing institutions (and not the CSPs) in order to safeguard the independence of the audits.*** ~~***performed jointly with other clients of the same cloud service provider in order to use audit resources more efficiently and to decrease the organizational burden both to clients and to the cloud service provider.***~~

(b) Third-party certifications and third party or internal audit reports made available by the cloud service provider provided that:

(…)

ii. The outsourcing institution thoroughly assesses the content of the certifications or audit reports ~~***continuously***~~*, in particular ensures that key controls are still covered in future versions of an audit report, and verifies* ~~***that***~~ *the certification or audit report* ~~**is not obsolete**~~**.**

(…)

iv. The certifications and audits are done against widely recognized standards ***which should be applied to both certifications and audit reports and assurance*** *and contain a test of operational effectiveness of the key controls in place.*

(…)

- The options regarding the right of audit should be limited to (i) pooled audits and (ii) third party certifications or audits performed by parties independent from the CSP, avoiding the conflicts of interest that can arise from the use of internal audit reports made available by the CSP, that we deem to be a less effective way of control.

In any case, it is worth mentioning article 28 paragraph 3 h) of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), which provides that the processor contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller. Therefore, whether and to the extent personal data are uploaded in cloud systems, the CSPs cannot anyhow object or make burdensome the audit and/or the inspection proposed by controller or processor, given the mandatory and binding force, at European level, of the GDPR.

We understand this requirement as covering a situation where an outsourcing institution chooses not to make use of its own audit resource, rather than as an exclusionary clause preventing firms which possess in-house audit resources of making use of pooled audits or third-party certifications.

For further clarity, the current wording should be replaced by the following: *"Where an outsourcing institution does not employ its own audit resources or where to do so would be impractical, it should at least consider one of the following tools:"*

- **Pooled Audits:** Onus should be on CSPs to provide audit, not outsourcing institutions. Although pooled audits could be possible within a community or sector (e.g. financial sector), when it comes to CSPs they would otherwise be prohibitively difficult to arrange. Further clarifications should be provided on how it could apply in practice as the concern remains that different supervisory authorities may understand this sentence in different ways.

  The following wording is therefore proposed (replacing the current wording in paragraph (a)):

  "(a) Execution of a third-party (p**ooled**) audit**s that is either executed by one of the participating outsourcing institutions or a trusted third-party, where the participating outsourcing institutions have the freedom to participate in determining the audit scope & where the audit is also paid by the outsourcing institutions (and not the CSPs) in order to safeguard the independence of the audits".

- **Third party certification:** We believe that the current requirement is not suitable and instead the burden should be on the CSPs to provide report and certification of their activities according to the requirements agreed.
  - Executing a full scope audit assignment on a major cloud provider's service offering would exceed the capabilities of the internal audit department within smaller or mid-size institutions thus creating a barrier to competition in financial services. It would also be difficult, and extremely costly, to identify a third-party with sufficient in-house expertise and execution ability to successfully complete such assignments. Applying an individual approach towards assessing the CSP is also not efficient considering that many banks will use the same service, and the time they would need to invest in audit execution.
  - We therefore believe that the best approach would be for the CSPs to cover the core audit scope, addressing confidentiality, integrity, availability, privacy etc., primarily covered under third-party assurance reports.
  - CSPs will probably be reluctant, even unwilling, to allow unlimited scope expansions on third-party assurance reports and thus recommendation 8 (b) v. may lead to a blocking issue during contractual negotiations and a barrier to the use of cloud services by financial institutions. This should be therefore rephrased accordingly.

- The wording of b (ii) stating *'continuously'* and that *'key controls are still covered'* or *'not obsolete'* should be defined further or deleted to avoid leaving room to legal uncertainties.

  The following wording is therefore proposed:

  "(ii) The outsourcing institution thoroughly assesses the content of the certifications or audit reports, in particular ensures that key controls are still covered in future versions of an audit report, and verifies the certification or audit report.

- The wording of 8(b)(iv) should be clarified by means of examples, by adding after '*recognized standards'*: *"which should be applied to both certifications and audit reports and assurance".*

  The following wording is therefore proposed:

  "iv. The certifications and audits are done against widely recognized standards ***which should be applied to both certifications and audit reports and assurance*** *and contain a test of operational effectiveness of the key controls in place".*

PARAGRAPH 9:

Suggestion for amendment:

~~***9. Considering that cloud solutions present a high level of technical complexity, the outsourcing institution should verify that the staff performing the audit – being its internal auditors or 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 audit and/or assessment of cloud solutions.***~~

We strongly advise the deletion of the entire paragraph because the Qualification of an Internal Audit function is ensured internally. It is indeed unclear how this paragraph will apply in practice (what is expected from a bank to ensure compliance? do the auditors require CISA, CCSK, CCSP or similar certifications and/or auditing skills, or does this imply deep technical expertise into every area of the cloud service?). The Qualification of external auditors is guaranteed via contractual obligations.

Keeping the present requirement will limit the use of cloud services to their full potential by financial institutions and will also restrict the type of application and service to be brought to the cloud. It will then create an uneven playing field, having a detrimental effect on competitiveness against those players that are not at all regulated.

It is also important to stress the difficulties linked to the intensive usage of new and sometimes proprietary technologies. Most banks face a huge challenge in finding the necessary expertise both in-house as well as on /outside the market.

It is not uncommon that banks are compelled to resort to recruiting staff that lack expertise or experience and train them on the job.

ADDITIONAL POINTS TO BE INCLUDED

- More requirements should be added into a special chapter entitled *'Access and audit rights'* by institutions. One recommendation is to add the requirement for CSPs to answer in a reasonable time period (no more than X *(number to be defined)* weeks from receiving the security assessment questionnaire and not later than X *(number to be defined)* weeks before entering into production) in an audit/security assessment questionnaire sent by the institution/bank (which needs to evaluate the risks in time, the vulnerabilities to be addressed and the risks to be reduced, if any).
- Among the rights, the economic aspects related to the execution of an audit should be introduced. Audits should be executed free of charge (or under a certain amount per year). Otherwise, as experienced, the CSP could ask the client to pay a disproportionate amount of money for it, making the right not achievable. Certain banks have experienced that certain CSPs stated that this would most likely be waived, if banks would share results with other banks using the service (which remains to be negotiated on a case-by-case basis).
  In this perspective, a joined/pooled audit as suggested above which is also non-chargeable may be a win/win solution for both banks and CSPs.

FOR COMPETENT AUTHORITIES

PARAGRAPH 10

Suggestion for amendment:

*(a) to provide to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) full access to the cloud service provider's business premises (head offices and operations centers **or other relevant offices**), including in the full range of devices, systems, networks and data used for providing the services to the outsourcing institution (right of access);*

- There should not be a restriction to only head office and operations center. The reference to "other relevant offices" should be added within the brackets. This is particularly problematic in case of use of SaaS of CSPs that are based outside Europe. For example, for certain CSPs it is not possible to geolocalise data within EU territory.
- It is not possible to allocate cloud data to certain locations; given this element the described monitoring (full access) will not cover the appropriate risks.

  The following wording is therefore proposed:

  *"a) to provide to the competent authority supervising the outsourcing institution (or any third party appointed for that purpose by that authority) full access to the cloud service provider's business premises (head offices and operations centers **or other relevant offices**), including in the full range of devices, systems, networks and data used for providing the services to the outsourcing institution (right of access);"*

CHAPTER 4.5 - SECURITY OF DATA AND SYSTEMS

- We consider that confidentiality of information, security, continuity and data location and processing are issues already covered by specific regulations (e.g. obligations resulting from the General Data Protection Regulation, NIS Directive) with which both financial institutions and CSPs will comply with.

  Therefore, this recommendation should refer to those regulations and avoid setting any additional requirements to those already established by the regulations in these areas.

  As a general comment, it is important to recall that – in general – outsourcing institutions should not only classify their data, but have to keep internal registries also known as records of processing activities (Art 30 of the General Data Protection Regulation (GDPR)) with general information concerning the outsourcing institution and the CSP, purposes of the processing, categories of personal data used and perhaps recipients of this personal data and descriptions of their technical and organizational safeguards (Art 32 of the GPDR).
  Outsourcing institutions have to make sure that the service providers they use are complying with appropriate data protection standards, especially with the GDPR and provide them with certain guarantees regarding data protection/data safety measures. Indeed, outsourcing institutions may also be liable in case of deficiencies of their service providers.

PARAGRAPH 16

- In our view, further clarifications should be provided regarding paragraph 16 points (a) and (b) to know if this classification and selection process has to be seen as a requirement for material services or if it applies to any service even non-material ones.

PARAGRAPH 18

- Paragraph 18 requires to monitor the performance of activities and security measures, including incidents, as well as to take corrective actions. It is important to recall that banks are already obliged to comply with GDPR, NIS Directive, European Central Bank incident reporting framework (which started on the 11th of July) as well as national regulations. We observe an overlap with other regulations already asking for the exact same measures.

CHAPTER 4.6 – LOCATION OF DATA AND DATA PROCESSING

- As a general comment (already mentioned previously), we observe that in the EBA draft recommendations particular attention is given to the data processing and data storage location, which are referenced across the entire document notably in recommendations 2 (c), 10, 14, 19 and 20. In our view, it is unclear to what location of data it refers to, what data processing it entails and what level of detail is expected. This can be interpreted as a requirement to specify a continent (e.g. Europe), an economic area (e.g. EU), a country, a physical data centre address or even a physical disk within a cloud provider's infrastructure.

In our view, the existence of the global dimension of the outsourcing to cloud service providers and of the location of data, data processing and data transfer should be acknowledged, as we observe that it is often perceived in regulatory guidelines as constituting a problem (even to the extent that the service cannot be used in a banking context).

Overall, we believe this high focus on data location in the EBA draft recommendations is not adapted to a reality where, already today and even more in the future, technology is expected to evolve and to affect the physical location of data, which will become less and less easy to identify because of its global dimension.

For example, readable data chunks are sliced, encrypted and stored across different systems in different geographical regions of the world. When logins and authorisations against a cloud service take place all the time in a multinational organisation, it may be beneficial to replicate information globally in every continent in order to keep the performance of the system intact and this is considered as a strength from a purely information security perspective.

This approach is already implemented as part of mainstream cloud technology with some of the world's largest CSPs. CSPs services are indeed for most of them "globalized", meaning they are transferring and collecting clients' data no matter where the data is, since some of the main providers of cloud services are either based outside the EU or use infrastructure outside the EU.

Therefore, personal data uploaded to the cloud is very likely to be transferred to entities located outside the EU. For example, some data are stored in the EU or in China etc., but some cloud directory and identity management service manage the request by transferring it to the USA.

- In order to avoid different interpretations being applied by different supervisory authorities, we would recommend becoming more specific on what the minimum requirements would be, without setting new requirements, considering that geolocalisation issues fall notably within the scope of regulations on data protection. Art. 28 (1) of the new General Data Protection Regulation 679/2016 provides indeed that controllers must only use processors providing sufficient guarantees *"to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject".*
- We would prefer to leave it to the banks themselves to assess and decide where data is stored based upon an internal risk-assessment. Global data storage should be a valid option in situations where the advantages outweigh the disadvantages.

CHAPTER 4.7 – CHAIN OUTSOURCING

PARAGRAPH 21

***"The outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider"*:**

Suggestion for amendment:

21. *As stated in guideline 10 of the CEBS guidelines, institutions should take account of the risks associated with "chain" outsourcing where the outsourcing service provider subcontracts elements of the service to other providers.* ***~~The outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider.~~ The outsourcing institution should be able to rely on the outsourcing service provider to perform the due diligence process of the subcontractor. Contractual procedures must be put in place for the CSP to ensure compliance with CEBS guidelines & GDPR requirement.*** *Furthermore the outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing agreement.* ***The list of subcontractors used by the CSP must be published to the outsourcing institution.***

- The text as currently drafted implies that it is the responsibility of the outsourcing institution to ensure that the subcontractor fulfills its contractual obligations with the contracting CSP. In our view, this is unworkable in practice. We believe that due diligence, risk assessments, controls and checks should be conducted by the CSP to ensure that all the subcontractors meet the security warranties to comply with the provisions mentioned in the contract.
  It means that the outsourcing institution should be able to rely on the outsourcing service provider to perform the due diligence process of the subcontractor.
  - As an example, we observe that a lot of services provided by certain CSPs' market places involve organisations which offer software and other cloud services, interesting for the bank running on the CSP cloud infrastructure. The contractual relationship that would be established when using such a service would be established between the bank and the organisation which is directly part of this CSP's Market Place (and not with the CSP itself). It will be next to impossible for the smaller players to impose the requirement above on large CSPs. Therefore, the subcontractor (the initial CSP) will most likely not comply with the current obligation proposed in recommendation 21 and therefore the recommendation should be amended by deleting the sentence *"The outsourcing institution should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider."* and replacing it by *"The outsourcing institution should be able to rely on the outsourcing service provider to perform the due diligence process of the subcontractor."*

In addition, the draft recommendation should be amended at the end of the paragraph by adding the following sentence: *"The list of subcontractors used by the CSP must be published to the outsourcing institution.*

- According to a similar reasoning under the GDPR, the initiator/outsourcer has to give its prior written consent for subcontracting (even if this could affect the service provision of the service provider), if personal data is being transferred. Under the GDPR this consent can also be provided in general for multiple sub-processors. The recommendation should therefore be amended by mentioning the following sentence *"Contractual procedures must be put in place for the CSP to ensure compliance with CEBS guidelines & GDPR requirement".*
- There are probably quite a few other scenarios where such a requirement may either not be possible or would be very impractical. As stated in the conclusion below, this may lead to blocking issues for cloud adoption, also depending upon how strict an interpretation will be given to this guidance by a regulatory authority.

The following wording is therefore proposed:

"21. As stated in guideline 10 of the CEBS guidelines, institutions should take account of the risks associated with "chain" outsourcing where the outsourcing service provider subcontracts elements of the service to other providers. ***The outsourcing institution should be able to rely on the outsourcing service provider to perform the due diligence process of the subcontractor. Contractual procedures must be put in place for the CSP to ensure compliance with CEBS guidelines & GDPR requirement.*** *Furthermore the outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing agreement.* ***The list of subcontractors used by the CSP must be published to the outsourcing institution."***

PARAGRAPH 23

"The notification period for those changes should be pre-agreed contractually to allow the outsourcing institution to carry out a risk assessment to consider the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect."

Suggestion for amendment :

23. The outsourcing agreement should also include an obligation for the cloud service provider to inform the outsourcing institution on any proposed significant changes to the subcontractors or the subcontracted services named in the initial agreement, which may affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. The notification period for those changes should be contractually pre-agreed ***so that the outsourcing institution can decide on*** ~~***to allow the outsourcing institution to***~~ *carry****ing*** *out* ***or not*** *a risk assessment to consider the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect.* ***An early termination clause should be included in the contract to allow the outsourcing institution to exit the contract in case it disagrees with the appointment of a new sub-contractor.***

- We very much welcome the approach of the EBA to provide that subcontracting requires ex ante notification to the outsourcing institutions. We indeed believe that further obligations should be imposed to the CSPs, such as a duty to inform the outsourcing institution of any changes related to the subcontractor or the subcontracted services which may affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. A notification period informing the outsourcing institutions about the changes before the subcontractor takes over, should be agreed among the CSPs and the outsourcing institutions, to allow the parties to assess the impact the changes may have on their activities.

- In our view, it is however not clear if this risk assessment is optional for the outsourcing institution or, on the contrary, if there is an obligation for the outsourcing institution to perform this new risk assessment. Section 3, paragraph 12 of the draft EBA recommendations mentions that the option was taken not to include the requirement for consent of the outsourcing institutions when the cloud service provider intends to change subcontractors. According to the draft recommendations it would otherwise be overly burdensome from a practical perspective in the context of cloud outsourcing as subcontracting is used extensively, the cloud environment is more dynamic than traditional outsourcing environments, and cloud services are provided to a larger number of clients than traditional outsourcing and on a larger scale. We believe that outsourcing institutions should keep the ability to establish their own criteria and provisions to ensure that subcontracting by CSPs has no effects on the conditions of the outsourced service. In practice, it is extremely difficult for financial institutions to have control of the whole outsourcing chain.

  Thus, the ability to assess the risk impact of the chain outsourcing should be an option contractually agreed, which the outsourcing institution decides to invoke or not.

  As rightly mentioned by the EBA in '*Chapter 5.1 Draft cost-benefit analysis / impact assessment'* paragraph *'D. Assessment of the technical options'* section on *'Exhaustive and prescribed list of requirements vs. non-exhaustive list'*, outsourcing institutions should *"retain the right to terminate the contract if the planned changes of subcontractor or subcontracted services will have an adverse effect on the risk assessment of the outsourced services".*

  An early termination clause should be therefore included in the contract to allow the outsourcing institution to exit the contract in case it disagrees with the appointment of a new subcontractor. Indeed, outsourcing institutions would not have the possibility otherwise to ensure that CSPs fulfil the requirements imposed by the NCAs.

  Alternatively, assessing and having the possibility to audit subcontractors when they contribute materially to the service performed could be considered as an option. For example, a presumption of materiality of 25 %.

The following wording is therefore proposed:

"23. The outsourcing agreement should also include an obligation for the cloud service provider to inform the outsourcing institution on any proposed significant changes to the subcontractors or the subcontracted services named in the initial agreement, which may affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. The notification period for those changes should be contractually pre-agreed ***so that the outsourcing institution can decide on*** *carry****ing*** *out* ***or not*** *a risk assessment to consider the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect.* ***An early termination clause should be included in the contract to allow the outsourcing institution to exit the contract in case it disagrees with the appointment of a new sub-contractor."***

CHAPTER 4.8 - CONTINGENCY PLANS AND EXIT STRATEGIES

Provisions of paragraphs 26 and 27 require the outsourcing contracts to include: *(a) "a termination and exit management clause which allows the activities being provided by the outsourcing service provider to be transferred to another outsourcing service provider or to be reincorporated into the outsourcing institution"* (par.26) and (b) *"an obligation on the cloud service provider to orderly transfer the activity and that of the subcontractors to another service provider or to the direct management of the outsourcing institution in case of the termination of the outsourcing agreement"* (par.27).

Those provisions are quite standard in outsourcing contracts, where the outsourcer manages (and often designs) the outsourced activities along with all the related technical infrastructure. In the case of cloud services, the applications themselves are managed, configured and (in particular for IaaS and PaaS) installed by the users (i.e. the outsourcing institution). In this context, these two provisions – when they refer to the transfer of activities from the CSP to another subject - risk not being applicable, since the outsourcing of own institution's activity based on the cloud service is still directly managed by the users.

In our opinion, termination and exit management clauses should ensure to the outsourcing institution the time necessary to transfer its applications and/or data to its new (internal or outsourced) infrastructure, as well as constant and unimpeded access to its data for the entire duration of the contract (including possible extensions to allow for the transfer of the activities).

PARAGRAPH 27

Suggestion for amendment:

(a) Develop and implement exit plans that are comprehensive, documented ***and sufficiently*** ~~***tested***~~ ***analysed*** *where appropriate*

Depending upon the interpretation of the sentence, this may become a de-facto blocker for cloud adoption. We would suggest clarifying this sentence further in order to ensure consistency among national supervisory authorities.

Depending upon how the recommendation is interpreted, this may rapidly become unworkable in practice. When we look at the experiences with specific software in certain banks, the on-boarding takes a significant amount of time and all the way this exit scenario is impossible. Any exit, out of the cloud service (either to on-premise, or to another provider), involves careful planning, data-capacity-network analysis, setting up migration structures and governance models (project/program), increase of staffing, purchasing of IT systems, temporary upgrade of network bandwidth etc.

Therefore, the exit strategy, in which various different scenarios have been considered, each with its drawbacks and benefits, is not fully testable.

We would therefore advocate to refer to 'sufficiently analysed' instead of 'sufficiently tested' in order to a have a more precise wording and avoid legal uncertainties.

It does seem feasible to perform exit planning exercises and table-top tests designed to identify weaknesses and attention points, if such an exit scenario is invoked. A high-level hierarchical escalation process up to where the decision can be made to activate the exit plan would also make it clear that this situation has been thought through.

But if this implies setting up on-premise infrastructure and regularly testing the technical exit process, then this measure would again be prohibitive where the cost of the exit scenario becomes so high that the business case immediately becomes void (a main reason to migrate to a cloud service is exactly so as not to have to set up any on-premise alternative).

In addition, further clarifications would be needed regarding the exact procedure needed to "orderly transfer the activity" in (c).

The following wording is therefore proposed:

*"(a) Develop and implement exit plans that are comprehensive, documented **and sufficiently analysed** where appropriate"*

PARAGRAPH 28

Suggestion for amendment:

~~d) Define success criteria of the transition.~~

The following sentence should be deleted: *"d) Define success criteria of the transition."* because the transition is successful if the retracted business processes operate duly (at the institution or at an alternative service provider). Requiring success criteria would be overburden some and/or redundant.

PARAGRAPH 29

Suggestion for amendment:

***29**. The outsourcing institution should include indicators that **~~can~~ could** trigger **~~the exit~~ a remediation plan / an audit ~~plan~~** in their ongoing service monitoring and oversight of the services provided by their cloud service provider.*

As the exit cannot be triggered by the crossing of a threshold, it would be relevant to monitor the performance and have an estimate of what level of performance is not acceptable. It should be up to each outsourcing institution to have a process that follows the Service Level Agreement (SLA) and could trigger this change.

The following wording is therefore proposed:

***"29**. The outsourcing institution should include indicators that **could** trigger **a remediation plan / an audit** in their ongoing service monitoring and oversight of the services provided by their cloud service provider".*

CHAPTER 5.1 – DRAFT COST-BENEFIT ANALYSIS / IMPACT ASSESSMENT – PARAGRAPH D

Suggestion for amendment:

Exhaustive and prescribed list of requirements vs. non-exhaustive list

(…)

*Secondly, the recommendations do not include specific requirements for reporting of security **or any other type** of incidents by institutions to their competent authorities in the context of cloud outsourcing. Since the topic of ~~**security**~~ incident reporting is broader than only for the context of cloud computing, the introduction of a more prescribed detailed recommendations would limit other potential security related issues outside the regulatory scope. It is therefore more reasonable to assess the topic outside the scope of the current draft recommendations but within **the scope of regulations already setting requirements on these topics (NIS, GDPR etc.)** ~~**the cybersecurity in general.**~~*

(…)

The recommendations explicitly exclude the handling of security alerts and security incidents. We however believe that it is an important point, especially in the context of the cloud where any attacks on the cloud provider might (or not) have an impact on the outsourced services (or "only" on outsourced services of other clients of the cloud provider). This will be known only if an attack is successful. In order to manage these risks actively and even prevent them, it is important for a bank to not only know of any security incidents, e.g. both while the incident is under analysis and after its closure, but also that an imminent threat is reported as soon as possible. An example: in case a threat is deemed to have a potentially high impact, banks might take banking services partially or completely off-line or might adapt security rules quickly to reduce the risk of a successful attack. This in a situation where nothing has happened so far.

In our view, the recommendations should expressly refer to the NIS Directive and favour a harmonisation of cybersecurity incident notifications to ensure a consistent approach.

As a suggestion for amendment, we encourage the EBA to take into account article 35 of the GDPR related to Data Protection Impact Assessment and to consider a CSP's obligation to carry out a risk assessment, even in a general way, to enable financial/outsourcing institutions to know and weigh the occurring risks of using a CSP as a service provider.

The following wording is therefore proposed in the second paragraph of section *'Exhaustive and prescribed list of requirements vs. non-exhaustive list'*:

*"Secondly, the recommendations do not include specific requirements for reporting of security **or any other type** of incidents by institutions to their competent authorities in the context of cloud outsourcing. Since the topic of incident reporting is broader than only for the context of cloud computing, the introduction of a more prescribed detailed recommendations would limit other potential security related issues outside the regulatory scope. It is therefore more reasonable to assess the topic outside the scope of the current draft recommendations but within **the scope of regulations already setting requirements on these topics (NIS, GDPR etc.)**"*

B. BASELINE SCENARIO

MANDATORY AND CONTRACTUAL CLAUSES

Regarding the provision *"capacity of the regulated institution to re-enter the data/ services",* further clarifications should be provided on what it means in practice and what *'re-enter'* means.

2. Are there any additional areas which should be covered by these recommendations in order to achieve convergence of practices in the context of cloud outsourcing?

FURTHER EDUCATION OF CSPs ON THE REQUIREMENTS THAT BANKS NEED TO FULFILL

Although CSPs are not subject to direct oversight by Financial Authorities, financial institutions are required to ensure in their outsourcing contracts that Competent Authorities can access and audit CSPs in relation to financial institutions' activities and according to article 55 of the Recovery and Resolution Directive can take control of the contract in case of bail-in.

Given that introducing these requirements into contracts with CSPs is usually burdensome for CSPs (which provide services also to entities other than financial institutions), the creation of a mechanism that guarantees that CSPs are aware of the requirements above and accept them, would ease the negotiation with CSPs and foster cloud adoption.

Moreover, this mechanism could also foresee the possibility of the CSP seeking a prior review by the Authorities, whose outcome would be an opinion on its capacity and adequacy to comply with financial regulation for different types of services. Should financial institutions intend outsourcing an activity that falls into a type of service for which Authorities have issued a positive opinion, this outsourcing could benefit from a "fast-track" notification/endorsement procedure.

We believe that, if this mechanism (e.g. voluntary CSP certification) were offered on an optional basis with voluntarily recourse to it by CSPs, no major changes on the regulatory framework applicable to CSPs and Financial Institutions would be necessary.

On the other hand, if the Authorities identify CSPs whose capacity/abilities do not allow the outsourcing institutions to comply with applicable financial regulation, their inclusion on a public blacklist of non-compliant CSPs would be very helpful for outsourcing institutions.

SYSTEMIC RISK

In our view, a description on how systemic risks (domestic, international) should be handled, is missing.

Third-parties' certifications are mentioned in paragraph 8(b) which would help financial institutions to rely on a standard approach across Europe. The adoption of base standard certifications to guarantee compliance or the definition of a cloud outsourcing banking standard against which a certification could be requested, would help financial institutions and CSPs across Europe to reduce the compliance burden and increase security. A more detailed reference to a base standard certification would help.

CYBERSECURITY: SECURITY INCIDENT MANAGEMENT & REPORTING

We suggest that the EBA recommendations clearly refer to existing regulation on security incident management and reporting (such as the NIS Directive) without adding new requirements or setting new criteria, so as to avoid overlaps with other regulations already requiring financial institutions and CSPs to report with different taxonomies, thresholds, etc. Examples are NIS, GDPR, PSD2, and ECB incident reporting framework or national regulations.

Furthermore, we believe that this consultation paper should emphasise that CSPs have to comply fully with the GDPR. In particular, CSPs should ensure that the tools and devices, on which the cloud services run, have been duly implemented so that service providers, and consequently the outsourcing institutions, are compliant with the GDPR provisions (including the security measures e.g. the provision of article 33 GDPR – *"Notification of a personal data breach to the supervisory authority"*).

DATA PROTECTION

It is important to reiterate that CSPs should ensure also that their tools and devices (on which the cloud services run) technically allow, without undue costs and burdens, the migration of the client's data to another CSP, upon client's request. Moreover, the CSPs have to collaborate and ensure the exercise of data subjects rights, as set forth in the GDPR (e.g. right to data portability, right to erasure), where the data subjects decide to exercise their rights towards data controllers (i.e. the outsourcing institutions).

Regarding the transfer of personal data and data localisation, we believe the European and National Supervisory Authorities should align with the decisions of the Data Protection Authorities (DPAs), if they have authorized transfer of data to certain countries complying with the GDPR.

As mentioned previously, we observe a certain overlap between local data protection laws, the future GDPR provisions for the protection of personal data and the requests made by national supervisors to perform risk analysis. We believe it is essential to take into account that data protection issues should be supervised by DPAs, on the basis of GDPR and local data protection laws. The NSAs should abide by the GDPR and the DPAs' decisions if they have granted permission to use a cloud service complying with all security and privacy measures. Decisions of the NSAs should not be stricter than the decisions of the DPAs as this would undermine the usage of the cloud and affect competition with other players that are not under the NSAs' supervision.

In addition, it is important to stress that, in order to ensure this level playing field, EU members' players should comply equally with regard to GDPR, but should not be forced to comply with extra requirements with regard to data protection, privacy and cybersecurity measures. Doing so would create a further competitive gap with non-European countries that face less friction to use the cloud.

STANDARD CONTRACTUAL CLAUSES DEFINED BY THE INDUSTRY

We observe that certain operating models of global CSPs conflict with requirements imposed on financial institutions as data controllers which creates additional challenges for the banking sector. For example, discrepancies are seen between the required timing of notice before sub-processor appointments and what the cloud providers consider as average.

The main impact for banks comes from the difficulty in agreeing to a contract covering open or undefined aspects of the service (such as data location), addressing various regulatory requirements from different regulators in jurisdictions where the contract is in force, and finding a CSP which can operate within EU regulations. Difficulties may occur without any reference to clear guidelines to negotiate contracts with large CSPs (which own global technology platforms accommodating large numbers of institutions in various jurisdictions). For example, banks might not be able to use cloud computing to its full potential because CSPs limit the use of cloud computing to a particular region.

Cloud services provided by external providers are currently handled according to existing legal requirements for outsourcing, defined by standard contracts issued by the CSPs. It is our understanding that, from a CSP perspective, due to the nature of the cloud service, a deep customisation to meet 100% the requirements of their customers is hardly feasible. Despite of the fact that CSPs usually pay attention to regulatory requirements of their customer's sector, Cloud Services Agreements are offered by most CSPs in standard, non-negotiable, "take it or leave it" terms. Such approach raises many concerns for the banking sector because the cloud service agreements proposed by the CSPs do not fully and adequately address the specific requirements imposed by European and national banking supervisory authorities with which banks have to comply.

For the banking sector, cloud adoption must be considered within the context of maintaining regulatory compliance. Outsourcing institutions/banks therefore typically approach compliance assurance with CSPs through specific contract clauses, Service Level Agreements (SLAs), certifications and audits. The lack of specific and detailed information drives banks and suppliers into a difficult situation: banks are generally forced to evaluate, on their risk assessment criteria basis, whether the provider solutions are adequate in terms of compliance (e.g. in terms of IT security). Banks have thus to make the choice of either rejecting the supplier or accepting the risks that cannot be fully mitigated.

This entire situation creates important barriers to the full adoption of cloud solutions by the banking sector as a whole.

Without limiting the CSPs' contractual freedom to negotiate specific conditions/clauses in line with their business model, the development, with the industry, of high-level principles covering the specific needs of the banking sector with the aim to also accommodate GDPR requirements, should be encouraged to guarantee legal certainty and facilitate the adoption of the cloud by financial institutions. For example, the contract between a bank and a CSP should include availability, reliability and confidentiality SLAs but leave open for the bank to decide which SLA to include.

For more information contact:

Noémie Papp
Senior Policy Advisor - Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69

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:

Noémie Papp
Senior Policy Advisor - Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69