Deutsche Bank

EU Transparency Register ID Number 271912611231-56

Deutsche Bank AG
Winchester House
1 Great Winchester Street
London EC2N 2DB

Tel +44 20 75458000
Direct Tel +44 20 75451903

24 September 2018

DB response to the European Banking Authority (EBA) Draft Guidelines on Outsourcing arrangements

Dear Sir or Madam,

Deutsche Bank welcomes the opportunity to provide comments on the Draft Guidelines on Outsourcing arrangements ("the guidelines").

We support the EBA's objective to align risk management practices for outsourcing arrangements across financial institutions in the EU. Divergent regulatory approaches should indeed be avoided, and in the face of digital and FinTech developments revising the guidelines drafted in 2006 is needed. In updating the framework for managing outsourcing risks, it is essential to maintain sufficient flexibility for EU financial services institutions to be able to react and adapt to market innovation. As technology continues to drive changes in business models over coming years, it will be important that these guidelines do not unduly constrain the ability of financial institutions to remain competitive.

With that in mind we would like to advise the EBA to avoid capturing too broad a range of services, or setting overly prescriptive requirements for the management of outsourcing risk. To that end, there are a number of areas within the proposed guidelines where further clarification or amendments to the drafting should be considered:

I. **Authorised activities:** Title II of the proposed guidelines sets out a range of conditions that must be met for the outsourcing of activities that require either authorisation or registration. As drafted, this section does not appropriately distinguish between the authorised activity as a whole and its sub-activities. A distinction is needed to avoid unnecessarily contraining the outsourcing of specific elements of processes or services which do not in themselves require authorisation or registration. This should be reflected in the final guidelines.

II. **Intragroup outsourcing:** The proposed requirements should take into account group governance and mitigation measures that are in place for intragroup outsourcing. A more balanced and proportionate approach should be considered in order to better reflect the benefits afforded by integrated risk management processes for these intragroup

arrangements. These benefits include, amongst others, required adherence of each subsidiary globally with group policies and standards on customer protection, risk management and controls.

III. **Criticality assessment:** the scope of outsourcing arrangements subject to enhanced requirements for critical or important functions should rely on the full assessment criteria set out in section 9.1 of the guidelines. In order to avoid straining supervisory and institutional resources, the guidelines should avoid capturing outsourcing arrangements linked to core business lines and critical functions which are low risk and not essential to the supported function.

IV. **Access and audit rights:** the requirement to secure 'necessary and effective' rights, as opposed to 'unconditional' rights, would better balance an appropriate level of supervision while removing potential barriers to the adoption of key outsourcing services by banks.

V. **Notification:** individual ex-ante notification would provide limited benefit to supervisory assessments of a bank's risk management of outsourcing arrangements. Ex-post information in combination with a focus on process and governance would be more effective in assessing outsourcing risks and risk management capabilities, and better address changes in technology and services.

Detailed responses to the specific questions asked in the consultation are set out in the attached annex. We would be happy to discuss these or any other points with the EBA as it finalises the draft guidelines.

Yours faithfully,

Matt Holmes
Head of Regulatory Policy

Annex 1 - Detailed response

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

Given the range of outsourcing arrangements which may fall under the updated guidelines, the need for national competent authorities to amend supervisory practices within existing rules, and the introduction of new requirements and resulting implementation of new processes / information gathering exercises required for compliance, the proposed application date of 30 June 2019 in paragraph 12 and transitional deadline of 31 December 2020 in paragraph 13 for the documentation of all existing arrangements would be extremely challenging to achieve.

As proposed, substantial time and considerable resources will be needed for outsourcing institutions to fully comply. This work may include potential changes to governance and internal policies, adjustments to or new builds of an institution's register, varying development lifecycles to update IT systems around potentially complex control systems and hold notices for any outsourcing projects in flight to verify compliance with the final guidelines. Importantly, a significant volume of work is expected related to the review of all existing outsourcing arrangements, and the potential need to update and negotiate contracts with service providers. These issues are further complicated by the fact that the proposed deadlines do not apply a risk-based or proportionate approach, as they require adherence to all provisions by the respective dates regardless of the critical or non-critical nature of the outsourcing.

It is our understanding that the final guidelines are expected to be published officially by the end of February 2019, leaving institutions with only four months before the guidelines apply. In order to provide sufficient time to implement the required changes, and to allow time for institutions to communicate with national competent authorities on any local considerations, we recommend the EBA revise the application date in paragraph 12 to 31 December 2019 at earliest.

The EBA should also consider a phased approach to compliance for existing arrangements, based on the potential risk impact of the outsourcing. Completion of documentation of critical and important outsourcing should be prioritised, while any existing, non-critical outsourcing service should not be considered as in scope for mandatory updates unless such contracts are subject to renewals or relevant amendments (typically undertaken every 2-5 years).

We therefore recommend that the transitional deadline of 31 December 2020 only apply to existing outsourcing arrangements deemed critical or important. Non-critical outsourcing arrangements would continue to be addressed according to their typical review and update cycle.

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

The alignment in section 2 of Title I of the guidelines, relating to outsourcing within group application with the EU Capital Requirements Directive / Regulation (CRD/R) is helpful, however, the proposed language infers that an outsourcing institution would be required to apply the EBA requirements in full to all entities, including third country entities within a group, unless foreign law expressly prohibits such measures. In order to avoid confusion over potential extra-territorial

reach, clarification is needed to confirm that the application of the guidelines are intended for authorised entities located in the EU. We therefore recommend that paragraphs 17 and 18 be amended as follows:

> *'17. Institutions and payment institutions* ***located in the EU*** *which are subsidiaries of an EU parent undertaking or of a parent undertaking in a Member State to whom no waivers have been granted on the basis of Articles 7 and 10 of Regulation (EU) No 575/2013 or of Article 21 of Directive 2013/36/EU should ensure that they comply with these Guidelines on an individual basis in accordance with Article 109 (1) of that Directive.'*
>
> *'18. In accordance with Article 109(2) of Directive2013/36/EU, these Guidelines should apply on the sub-consolidated and consolidated basis. For this purpose, the EU parent undertakings and the parent undertaking in a Member State should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries* ***located in the EU****, including payment institutions are consistent, well-integrated, and adequate for the effective application of these Guidelines at all relevant levels.'*

We welcome the clarity provided in paragraph 19, in conjunction with paragraphs 46 – 47 in section 8, that institutions within a group may rely on a centrally-maintained register as long as each institution can easily draw from the central register all relevant information required under the guidelines.

As drafted, however, paragraph 19(b) could be interpreted to imply that: i) each competent authority is expected to have 'their' own register, maintained at the institution; and ii) the EBA intends to regulate the relationship between non-EU subsidiaries and their non-EU supervisory authorities.

We believe that neither was the intention of the EBA as there is no need for such measures if there is a centrally maintained register from which timely extracts can be supplied. Therefore, to avoid potential confusion in the implementation of the final guidelines, we recommend that paragraph 19(b) be amended as follows:

> *'where the register of all existing outsourcing arrangements as referred to in Section 8, is established and maintained centrally within a group, the competent authorities, all institutions and payment institutions should be able to obtain* ***an extract from that register providing a view of those outsourcing arrangements (extra and intragroup) relevant to entities within their jurisdiction without undue delay.*** ~~*their respective individual register without undue delay and it should be ensured by the institution or payment institution that all outsourcing arrangements, including outsourcing arrangements with service providers inside the group, are included in their individual register.'*~~

The EBA also clarifies that intragroup outsourcing should be subject to the same regulatory framework as outsourcing to service providers outside of the group. The EBA acknowledges that intragroup outsourcing may allow for 'a higher level of control over the outsourced function which they could take into account in their risk assessment'. However, the requirements laid out in the guidelines imply that intragroup arrangements can be equal or even riskier than external

outsourcing, and in particular highlights concerns over potential conflicts of interest. These conflicts are not further specified or explained – especially in comparison to conflicts which may exist with a third party vendor – in the draft guidelines

While we support the application of the guidelines to intragroup arrangements, we are concerned that insufficient recognition is given to the benefits afforded by integrated risk management processes for intragroup arrangements nor the enhanced control framework available to service recipients. In comparison to outsourcing to third parties, these internal processes and controls result in a lower risk profile for intragroup outsourcing.

For example, in line with Articles 109(2) and 74 of the EU Directive 2013/36, each subsidiary within the group is required to operate in-line with globally applicable group policies and standards on customer protection, risk management and internal controls. Furthermore, the internal audit system is applied to all subsidiaries worldwide, with intragroup service documentation usually based on standardised contract templates centrally issued by the legal department. These benefits are present regardless of the location of the service provided, so third country intragroup providers should not automatically be assumed to be riskier than providers located within the EU.

In this regard, a differentiated approach should be applied which provides preferential treatment to intragroup outsourcing, in order to more accurately reflect the actual risk posed by these arrangements. The final guidelines should provide a more proportionate, risk-based approach which differentiates between third party and intragroup outsourcing, with regards to, but not limited to: the criteria for assessing criticality or importance; due diligence; preconditions for outsourcing to third country entities; and exit strategies.

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

We welcome the examples provided in paragraph 23 of activities which should not be considered outsourcing; however, it would be helpful to provide additional clarity by noting that the list in paragraph 23 is non-exhaustive. This should be complemented with a more detailed list of examples in the annex of the final guidelines, such as the list presented in the European Banking Federation's (EBF) response letter to the EBA.

As outsourcing is likely to play an increasingly important role in the financial system as new business models, partnerships and technologies gain traction, it would benefit both industry and competent authorities to ensure that only the services which pose risk to the outsourcing institution are subject to the updated guidelines. The EBA should therefore consider reviewing this list in cooperation with industry participants every two years and update as needed.

In regards to the requirements outlined in paragraphs 25 – 26 on the outsourcing of activities that require authorisation or registration by a competent authority in the Member State the institution is authorised, the current wording risks an overly restrictive approach which could

constrain the outsourcing of specific elements of processes or services for efficiency and operational reasons.

It would be useful to clarify that the restrictions and requirements in these paragraphs do not affect outsourcing of parts of banking activities which are subject to authorisation, but are instead limited to licensed activities themselves. For example, it is not clear why back office functions and processing / operational functions should not be outsourced to an entity that is not licensed for the entire activity or is located in a third country, as the licensed activity still remains under control of the institution. This is especially relevant in the context of payment or securities settlement activities, where outsourcing to intragroup or external ancillary service providers is very common. An institution may also be required to retain a service provider in a third country for cross-border business to partially support certain elements of the business, e.g. for KYC due diligence. We therefore recommend that paragraphs 25 and 26 be amended as follows:

> *'Without prejudice to the requirements within Title III, institutions and payment institutions should ensure that,* ***if*** *banking activities or payment services that require authorisation or registration by a competent authority in the Member State where they are authorised are* ***to be outsourced in full or to a material extent, that they are*** *only outsourced to a service provider located in…'*

Furthermore, we are concerned that the criteria set out in paragraph 26 for outsourcing arrangements in third countries will unnecessarily restrict the range of providers available to institutions. While we agree on the importance of the home supervisor's ability to supervise the outsourcing institution, the requirements in paragraph 26(b) applies a singular solution through the use of a formal memorandum of understanding (MoU).

Recognising that this requirement should only apply to the outsourcing of authorised banking activities or payment services in full or to a material extent (as per the above recommendation) and thus narrow the scope of impacted arrangements, limiting the supervisory mechanism to MoUs would nonetheless be problematic. This could restrict a range of countries where cooperation agreements are not yet available, where the timing of their finalisation is not known or where existing cooperation agreements may be revoked.

We believe a more suitable approach would be an outcomes-based one, as outlined on page 57 of the guidelines as a potential policy option, which relies on an institution's assessment that outsourcing to service providers in a third country would not prevent or undermine an EU national competent authority's ability to effectively supervise the outsourcing institution and their outsourcing arrangements. This would provide greater flexibility and certainty to institutions on the continued viability of service providers located in third countries, while maintaining effective supervisory capabilities.

If the guidelines however maintain the existence of an MoU as a precondition, the establishment and maintenance of a public register for MoUs by the EBA would also provide much needed transparency on cooperation agreements which meet the requisite requirements in paragraph 26. This would include updating and providing clarity to outsourcing institutions on scenarios where an MoU is withdrawn or amended.

Additionally, we recommend the EBA also provide relief from the requirements set out in paragraph 26 in the case of outsourcing to a service provider in third countries, when such

provider wholly belongs to the same group as the outsourcing institution. These entities would therefore be part of the organisational structure and subject to the risk management policies of the group. Intragroup contracts as well as group governance will ensure full compliance with the regulatory requirements of the service recipient. This could be addressed with the addition of a new paragraph 26(d):

> *'outsourcing to a service provider located in a third country that is wholly owned by an institution or payment institution and subject to the risk management policies and governance processes of the group would however be exempt from the requirements set out in paragraph 26(a), (b) and (c).'*

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

With regard to the governance arrangements set out in paragraph 32(g), in combination with requirements set out in paragraphs 89-91, such sections would expressly require for an alternative service provider or the ability to reintegrate an outsourced critical or important function, and to ensure such exit plans are comprehensive, documented and sufficiently tested.

While we generally agree and support such requirements, it is unclear how the proposed testing requirements would work in the case of complex services like a data centre outsourcing, where migration activities would require significant and complex planning efforts and typically take multiple years to complete. Exit plans are based on assumptions and 'moving targets', and are therefore hypothetical, i.e. cannot be 'tested' without actually a full effort of, for example, going to market with a second provider. Therefore, to better reflect such scenarios we propose to amend the 'testing' language in paragraph 90(a) with a requirement for comprehensive and plausible documentation as follows:

> *'develop and implement exit plans that are comprehensive and documented* ***in a plausible manner*** ~~***and sufficiently tested (e.g. by carrying out an analysis of the potential costs, impact, resource and timing implications of transferring an outsourced service to alternative provider) comprehensive, documented***~~*;'*

It is also worth noting that in certain circumstances the identification of a suitable alternative service provider is not always possible. As highlighted in the EBF's response letter, this may include the use of SWIFT and may in the future include certain innovative technologies which require specialised expertise. In such situations we believe the requirement in 32(g) should not immediately preclude the outsourcing arrangement, as long as a sufficient risk assessment is conducted and increased risk management measures are put in place to mitigate the relevant risks.

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

The guidelines reference the need to account for and manage conflicts of interest that may be caused by both external and intragroup outsourcing arrangements (e.g. para 38 and recitals 26 and 37). For intragroup arrangements, we assume that this conflict could arise from service

relationships between the back office (service provider) and the front office (client or outsourcing party).

In line with our response to Question 2, the guidelines' current language can be read to imply that outsourcing between entities within the same group may create special conflicts of interest which may not already be addressed under existing regulations or processes, and may require additional measures.

It is currently unclear what specific, unique scenarios and conflicts the EBA envisions within these intragroup arrangements – which are conducted at arm's length – which may require going beyond existing governance models and adherence to existing regulations. Additional clarity on this point would be appreciated.

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

We encourage the EBA to maintain a risk sensitive approach combined with the principle of proportionality throughout the final guidelines. This will be important from resourcing and burden standpoints for both supervisors and institutions, in order to ensure that outsourcing arrangements of highest importance are provided the necessary, enhanced attention and oversight.

We therefore agree with the need for enhanced documentation for outsourcing of critical or important functions, but believe the scope of covered outsourcing arrangements should rely on the full assessment criteria set out in section 9.1. To align the final guidelines with this objective, we recommend paragraph 47(c) be amended as follows in order to only apply to the outsourcing of critical or important functions:

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

Outsourcing to cloud service providers that are deemed critical or important would still be captured, based on the assessment criteria set out in section 9.1. This would however avoid an unnecessary increase in compliance burden for cloud services which do not require the application of enhanced requirements or scrutiny of both supervisor and institution.

This approach would also align with the EBA's intention to adopt a technological neutral and proportionate approach to regulation, as outlined in its FinTech Roadmap from 15 March 2018[1]. Of the three approaches outlined in the Roadmap, the first included reviewing existing EU measures and the ongoing monitoring of supervisory guidance.

We support the EBA's aim of promoting technological-neutrality in regulatory and supervisory practices and believe it should be applied wherever possible in the final outsourcing guidelines.

[1] https://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf

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

It is unclear what is expected from an outsourcing institution when considering whether a service provider is part of the institution's accounting consolidated group, as highlighted in paragraph 48(f), within the context of the pre-outsourcing analysis. It would be helpful to better understand what is required in practice if a service provider belongs to an institution's accounting consolidation group and how this may relate or impact a different type of risk appetite.

The current wording in paragraph 50 would benefit from refinement to better align the determination of a critical or important outsourcing with the full criteria set out in section 9.1, and reflect the relevant materiality of a specific arrangement.

The current approach unfortunately applies an overly broad lens where any potential activity, process or service (e.g. operational or administrative) that is potentially linked to a core business line or critical function – regardless of its relevance or materiality to the supported function – would be considered critical or important and be subject to the enhanced requirements of the guidelines. This approach ignores any sort of assessment of actual risk / importance and would result in the diversion of internal risk management and oversight resources to activities, processes or services with relatively low risks, as well as introduce unnecessary compliance burdens (e.g. enhanced documentation requirements) and costs to the outsourcing institution.

The EBA should instead focus on the full criteria that should be considered in determining if an outsourcing arrangement is critical or important and better reflect the relevance of the outsourcing. We therefore recommend paragraph 50 be amended as follows:

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

Regarding the specific assessment criteria included in paragraph 51(g) regarding 'scaling service consumption', we recommend that the final guidelines clarify that the assessment of scaling should specifically focus on unexpected changes to the contract which may result in a significant risk increase in connection with the outsourcing arrangement.

For example, scaling would not be a concern for outsourced services which operate on volume-based contracts and can in theory increase infinitum. Typically, the variation in these services cannot be predicted up front but are expected during the lifetime of the arrangement to occur. This is also true for outsourcing arrangements which are intended to be elastic. Service consumption flexibility as such does not in practice constitute a risk factor, as both parties usually work with volume models to cover expected costs as well as delivery capability. This actually

mitigates risks for the institution as it allows more cost controls and service flexibility to better react to changes in demand and markets.

A more suitable approach would be to focus on the potential risk increase from significant new volume or importance of the service without another contract review. We therefore recommend the EBA amend the language in paragraph 51(g) as follows:

> *'the possibility of the proposed outsourcing arrangement to be scaled up at the discretion of either party* ***in an unintended manner which would result in a significant increase in risk concentration to the outsourcing institution*** *without replacing or revising the underlying agreement;'*

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

No comments on this section.

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

The expectations regarding an institution's own risk assessment are sufficiently clear. However, certain considerations in the guidelines related to the political stability and security situation of the service provider's jurisdiction are overly prescriptive.

Specifically, the detailed requirements set out in paragraph 61(d) ii and iii would significantly increase legal costs and the time to market for outsourcing arrangements, without providing a material benefit to the overall risk assessment. This would require for example the provision of legal memorandums for every jurisdiction where a service provider is under consideration. While political stability and security is typical part of the vendor location risk, these requirements go beyond that risk focus.

In particular, the requirements in 61(d) iii, as well as paragraph 64(h) and (i), to consider 'any constraints' provides limited value even within Europe, where these rights can already be challenged under European insolvency laws by the insolvency receiver. Even EU insolvency laws will prevail over any bank regulation and therefore no vendor due diligence or any clause in an outsourcing service contract is able to change mandatory rights of an insolvency receiver, e.g. challenging existing contracts and payments in accordance with available rights.

Therefore, in order to more accurately reflect these insolvency scenarios, we recommend the EBA avoid prescriptive requirements in this area by removing items i-iii under paragraph 61(d) and paragraphs 64(h) and (i).

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

In order to avoid restricting the further development and use of electronic signatures, greater clarity on what can be considered a 'written agreement' in paragraph 62 would be beneficial. In particular, alignment with the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[2] should be secured to confirm the acceptance of advanced electronic signatures and further drive electronic execution of contracts in line with the technological progress in the area of digital contracting. This is increasingly important as the use of advanced electronic signatures will be a necessary element to satisfy secure electronic contracting processes going forward with a reasonable amount of implementation effort and sufficient technical security.

Conversely, any requirements for qualified electronic signatures for all outsourcing contract types would create significant burdens on the implementation of digital processes and should not be considered as proportional, in consideration of the intention of the eIDAS Regulation.

We therefore recommend the addition of a new definition for 'written agreement' under paragraph 11, as follows:

> *'means any contract document signed by authorised representatives of the involved parties either physically in writing or electronically, using advanced electronic signatures in accordance with the EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)'*

The requirements set out in paragraphs 63(h), 66(b) and 72(b) for the outsourcing institution to secure 'unrestricted' rights to access and audit the service provider and subcontractors for any outsourcing relationship will pose significant legal and practical challenges, as well as security concerns for both the outsourcing institution and service provider.

This will be particularly the case for providers of standardised services (e.g. cloud service providers) which also have a significant number of customers. While we fully agree that access and audit rights are essential for the monitoring and supervision of critical outsourcing arrangements, requiring *unrestricted* access to *any* outsourcing arrangement would unnecessarily overreach, introduce new risks to both sides of the outsourcing arrangement and potentially prevent the adoption of existing and potentially new outsourcing arrangements in the developing financial services ecosystem.

This requirement also exceeds approaches employed by regulators in other jurisdictions, which require securing a necessary or suitable right to access, to allow for appropriate supervision of the outsourced activity. Policymakers and supervisors are increasingly adapting their frameworks to reflect these challenges in the face of technological and business model changes.

For example, the UK Financial Conduct Authority (FCA) requires that 'the firm, its auditors, the FCA and any other relevant competent authority must have **effective access** to data related to the outsourced activities, as well as to the business premises of the service provider; and the FCA

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

and any other relevant competent authority must be able to exercise those rights of access'[3]. This same 'effective access' approach is included in Article 31(2)(i) of the MiFID Org Regulation.

Similarly the U.S. Office of the Comptroller of the Currency's (OCC) Risk Management Guidance requires that the bank 'ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified'[4].

Similar, more flexible approaches are employed in both the U.S. and APAC, which do not impose such unconditional and potentially inoperable requirements for outsourcing arrangements (see Annex 2 for examples of specific regulatory language).

Amending the language in the EBA guidelines to achieve a more feasible and proportionate standard is especially important, as this will apply to not only all outsourcing arrangements, but also any sub-outsourcing. A consistent approach across jurisdictions will also better support the smooth functioning and central risk management of outsourced arrangements for large, globally active financial institutions and the scaling of innovative solutions in a responsible and controlled manner.

We therefore recommended that paragraph 63(h) be amended as follows:

> *'the **~~unrestricted~~** **necessary and effective** right of institutions, payment institutions and competent authorities to get any information needed with regard to the outsourcing and to access and audit the service provider as further specified in Section 10.3;'*

Paragraph 72(b) would similarly be amended as follows:

> *'**~~unrestricted~~** **necessary** rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to **effectively** monitor the outsourcing arrangement and to comply with all applicable regulatory requirements.'*

The guidelines also introduce a significant, disproportionate change to the current approach on non-critical outsourcing requirements by requiring specific contract content for these non-critical services without respecting an informed, risk-based view. It is especially challenging to expect unlimited or unrestricted audit and inspection rights in a contract with a non-critical service provider. This issue is further complicated by the broad outsourcing definition applied in the guidelines – which may now include all kinds of activities to be covered by an extensive outsourcing arrangement – instead of a risk-based content.

Therefore, we recommend to at least limit the audit clause requirements of paragraph 63 (g) and (h) as well as Section 10.3 to critical and important functions, and otherwise refer the applicability for non-critical services to the extent required by the institution for its effective risk management.

We also encourage the EBA to consider a more proportionate and forward-looking approach on sub-outsourcing / chain outsourcing. As highlighted in our response to the EBA's recommendations on cloud outsourcing in 2017, it is extremely difficult for a financial institution to have control of a cloud service provider's whole outsourcing chain, due to the more dynamic

[3] https://www.handbook.fca.org.uk/handbook/SYSC/8/1.html
[4] https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

nature of the cloud environment and larger volume of customers than what is found in traditional outsourcing environments.

We therefore recommend the EBA to accept alternatives to direct firm oversight which would more effectively address the identified risks and nature of dynamic sub-outsourcing. For example, in a recent report released by U.S. Treasury on regulatory reforms to promote innovation[5], the Treasury recommended that supervisors formally recognise independent audit and security standards that sufficiently meet regulatory expectations and set clear and appropriately tailored expectations for chain outsourcing. This was done in order to provide for a 'prudent and informed migration of activities to the cloud'. The adoption of such alternative solutions and oversight mechanisms for compliance of sub-outsourcing, such as the requirements in paragraph 66 and the due diligence standards set out in section 9.2, would better enable the adoption of cloud services for financial institutions and better future-proof the guidelines to changes in technology and the financial services landscape.

The requirements in paragraph 76 set out the need for the outsourcing institution to ensure its ability to carry our security penetration testing to assess the effectives of implemented cyber and internal ICT security control and mitigation measures. This is an important area of risk management and will be increasingly so as the financial services sector continues its current wave of digital transformation.

However, this requirement can be read to require that each outsourcing institution secure the right to conduct their own individual penetration testing (whether by internal staff or external experts) on the service provider's systems.

While the requirement to conduct penetration testing is not a new concept or standard, the potential application of such a narrow approach where only the outsourcing institution can conduct the testing may be inoperable in practice and create extensive security issues for both the outsourcing institution and service provider. This again is especially true for standardised services such as cloud services. For example, a scenario where every customer of a large cloud service provider – whose customers can number in the hundreds of thousands – is entitled to conduct penetration testing would create significant operational complexity and increase risks of data exposure, corruption, theft and leakage, as well as potential denial or disruption of service and performance issues for other customers.

A more secure and workable approach would be to clarify that the outsourcing institution can meet the requirement for security penetration testing through a number of methods. Current best practice includes offering alternatives to direct client testing, such as acceptance of reports from reputable third parties or to offer assistance to jointly conduct the testing alongside the service provider. This would be in the same spirit as the flexibility provided in paragraph 75 for pooled audits, and similarly decrease the operational burden on, and risks for, both the client and the service provider. The language in paragraph 76 should be amended to reflect such an approach as follows (edits in bold):

> *'In line with the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process institutions should, where relevant, ensure the*

[5] https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf

ability to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes. Taking into account Title I, payment institutions should also have internal ICT control mechanisms, including ICT security control and mitigation measures. ***The outsourcing institution may meet this requirement by acquiring reasonable evidence on the security, either directly or by the vendor, through an external tester, and perform the test under their control.*** *'*

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

No comments on this section.

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

No comments on this section.

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

We agree with the need to harmonise requirements across markets participants but recommend the EBA consider industry best practices for the process and manner of reporting material outsourced activities to competent authorities.

For example, under the German Banking Act, the outsourcing institution includes information on outsourcing activities in its audit reports. This arrangement has worked well to date in Germany for both the financial institution and regulator in carrying out appropriate risk management and supervisory tasks; a separate or standalone notification, which was previously utilised, has not been deemed necessary or efficient for the accomplishment of these tasks.

This ex-post approach still provides the right of the supervisor to request unwinding (or amendments of) any outsourcing arrangement that would not comply with the national rules set up under the guidelines. Furthermore, certain information required for notification is usually not available until after negotiations have been finalised, e.g. outsourcing agreement reference number. In other situations, information might only be available if negotiations are in a very advanced stage.

The need for ex-ante notification would not only increase the time to market of outsourcing arrangements and add additional operational burdens and costs, but would do so without

providing additional value to the supervisor looking at the overall strategy of an institution, including generally implemented risk control functions.

A more efficient approach to ensuring appropriate due diligence and assessments are completed prior to proceeding with an outsourcing arrangement, would be for regulators to focus on the robustness of an institution's internal governance and control frameworks. Assessing an institution's processes would address the execution of appropriate risk management practices for outsourced activities, which are necessary for adapting to the development of new and more complex levels of services and technologies, e.g. in the cloud environment.

In short, focusing on process and governance would be more effective as process equals outcome. This would better position the EBA and local supervisors to account for the rapidly evolving technological landscape, subsequent changes in outsourcing arrangements and potential new providers.

However, if the EBA is intent on mandating ex-ante notification, this should only require a brief summary of the outsourcing arrangement and should not be subject to pre-authorisation from the competent authority.

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

No comments on this section.

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

No comments on this section.

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

No comments on this section.

Annex 2: Outsourcing approaches on rights of access and audit

Regulator	Jurisdiction	All v. Material Outsourcing	Text
Office of the Superintendent of Financial Institutions (OSFI) Outsourcing of Business Activities, Functions and Processes [6]	Canada	Material	**7.2.1 Contract for Services** *f) Ownership and Access* Identification and ownership of all assets (intellectual and physical) related to the outsourcing arrangement should be clearly established, including assets generated or purchased pursuant to the outsourcing arrangement. The contract or outsourcing agreement should state whether and how the service provider has the right to use the federal regulated entity's (FRE) assets (e.g., data, hardware and software, system documentation or intellectual property) and the FRE's right of access to those assets. *h) Audit Rights* The contract or outsourcing agreement is expected to clearly stipulate the audit requirements and rights of both the service provider and the FRE. At a minimum, it should give the FRE the right to evaluate the service provided or, alternatively to cause an independent auditor to evaluate, on its behalf, the service provided. This includes a review of the service provider's internal control environment as it relates to the service being provided. In addition, in all situations, irrespective of whether an activity is conducted in-house, outsourced, or otherwise obtained from a third party, OSFI retains its supervisory powers. Accordingly, an undertaking from the service provider or a provision in the outsourcing contract, should give OSFI or the Superintendent's representative the right to: • exercise the contractual rights of the FRE relating to audit; • accompany the FRE (or its independent auditor) when it exercises its contractual audit rights; • access and make copies of any internal audit reports (and associated working papers and recommendations) prepared by or for the service provider in respect of the service being performed for the FRE, subject to OSFI agreeing to sign appropriate confidentiality

[6] http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx

			documentation in form and content satisfactory to the service provider; and • access findings in the external audit of the service provider (and associated working papers and recommendations) that address the service being performed for the FRE, subject to the consent of the service provider's external auditor and OSFI agreeing to sign appropriate confidentiality documentation in form and content satisfactory to the service provider and the external auditor. OSFI would provide the FRE with reasonable notice of its intent to exercise its audit rights and would share its findings with the FRE where appropriate. In the normal course, OSFI would seek to obtain information it requires through the FRE itself.
Hong Kong Monetary Authority (HKMA) Supervisory Policy Manual SA-2: Outsourcing [7]	Hong Kong	All	**2.8 Access to outsourced data** 2.8.1 AIs Authorized Institutions (AIs) should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA in accordance with §§55 and 56 of the Banking Ordinance and that data retrieved from the service providers are accurate and available in Hong Kong on a timely basis. 2.8.2 Access to data by the HKMA's examiners and the AI's internal and external auditors should not be impeded by the outsourcing. AIs should ensure that the outsourcing agreement with the service provider contains a clause which allows for supervisory inspection or review of the operations and controls of the service provider as they relate to the outsourced activity.
Australian Prudential Regulation Authority (APRA) Prudential Standard CPS	Australia	Material	**APRA access to service providers** 34. An outsourcing agreement must include a clause that allows APRA access to documentation and information related to the outsourcing arrangement. In the normal course, APRA will seek to obtain whatever information it requires from the APRA-regulated institution; however, the outsourcing agreement must include the right for APRA to conduct on-site

[7] https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf

231: Outsourcing [8]			visits to the service provider if APRA considers this necessary in its role as prudential supervisor. APRA expects service providers to cooperate with APRA's requests for information and assistance. If APRA intends to undertake an on-site visit to a service provider, it will normally inform the APRA-regulated institution of its intention to do so. 35. Where an APRA-regulated institution enters into an outsourcing arrangement with a related body corporate, the APRA-regulated institution must ensure that access by APRA to the related body corporate is not impeded. 36. An APRA-regulated institution must take all reasonable steps to ensure that a service provider will not disclose or advertise that APRA has conducted an on-site visit, except as necessary to coordinate with other institutions regulated by APRA that are existing clients of the service provider.
Monetary Authority of Singapore (MAS) Guidelines on Outsourcing [9]	Singapore	Material	**5.9 Audit and Inspection** 5.9.1 An institution's outsourcing arrangements should not interfere with the ability of the institution to effectively manage its business activities or impede MAS in carrying out its supervisory functions and objectives. 5.9.2 An institution should include, in all its outsourcing agreements for material outsourcing arrangements, clauses that: a) allow the institution to conduct audits on the service provider and its subcontractors, whether by its internal or external auditors, or by agents appointed by the institution; and to obtain copies of any report and finding made on the service provider and its subcontractors, whether produced by the service provider's or its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractor, in relation to the outsourcing arrangement;

[8] https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf
[9]http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf

			b) allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the institution to: i. access and inspect the service provider and its sub-contractors, and obtain records and documents, of transactions, and information of the institution given to, stored at or processed by the service provider and its sub-contractors; and ii. access any report and finding made on the service provider and its sub-contractors, whether produced by the service provider's and its sub-contractors' internal or external auditors, or by agents appointed by the service provider and its sub-contractors, in relation to the outsourcing arrangement.
Financial Conduct Authority (FCA) Senior management arrangements, Systems and Controls [10]	UK	All	**8.1 General outsourcing requirements** 8.1.8 (9) the *firm*, its auditors, the *FCA* and any other relevant *competent authority* must have effective access to data related to the *outsourced* activities, as well as to the business premises of the service provider; and the *FCA* and any other relevant *competent authority* must be able to exercise those rights of access.
Federal Financial Supervisory Authority (BaFin) Minimum Requirements for Risk Management [11]	Germany	Material outsourcing	**AT 9 Outsourcing** 6 The following terms shall be agreed in the outsourcing contract for material outsourcings: a) specification and if necessary description of service to be performed by the insourcing company, b) stipulation of information and audit rights of the internal audit and external audits, c) ensuring BaFin's information and examining rights and control capabilitiy, d) rights to give directives if necessary, e) regulations that ensure compliance with data protection provisions,

[10] https://www.handbook.fca.org.uk/handbook/SYSC/8.pdf

[11] https://www.bundesbank.de/Redaktion/EN/Downloads/Tasks/Banking_supervision/PDF/minimum_requirements_for_risk_management_mindestanforderungen_an_das_risikomanagement_marisk.pdf?__blob=publicationFile

			f) appropriate periods of notice, g) regulations on the possibility and the modalities of sub-outsourcing that guarantee that the institutions continue to comply with the banking supervisory requirements, h) the commitment of the insourcing firm to inform the institution of any developments that may impair the proper performance of the outsourced activities and processes. 7 The institution shall manage the risks associated with material outsourcings in an appropriate manner and monitor the execution of the outsourced activities and processes in a proper manner. This also includes a regular evaluation of the service of the insourcing firm on the basis of specific criteria. The institution must assign clear responsibilities for management and monitoring.
Federal Reserve (Fed) Guidance on managing Outsourcing Risk [12]	USA	All	**C. Contract Provisions and Considerations** Right to audit: Agreements may provide for the right of the institution or its representatives to audit the service provider and/or to have access to audit reports. Agreements should define the types of audit reports the financial institution will receive and the frequency of the audits and reports.
Office of the Comptroller of the Currency (OCC) OCC Bulletin 2013-29: Third Party Relationships - Risk management Guidance [13]	USA	All	**The Right to Audit and require remediation** Ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews). Consider whether to accept audits conducted by the third party's internal or external auditors. Reserve the bank's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits. Audit reports should include a

[12] https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf
[13] https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

			review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.
Office of the Comptroller of the Currency (OCC) OCC Bulletin 2017-21: Frequently asked questions to supplement OCC Bulletin 2013-29 [14]	USA	All	**14. Can a bank rely on a third party's Service Organization Control (SOC) report, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18)?** In meeting its due diligence and ongoing monitoring responsibilities, a bank may review a third party's SOC report prepared in accordance with SSAE 18 to evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls.4 If a third party uses subcontractors (also referred to as fourth parties), a bank may find the third party's SSAE 18 report particularly useful, as SSAE 18 requires the auditor to determine and report on the effectiveness of controls the third party has implemented to monitor the controls of the subcontractor. In other words, the SSAE 18 report will address the question as to whether the third party has effective oversight of its subcontractors. A bank should consider whether an SSAE 18 report contains sufficient information and is sufficient in scope to assess the third party's risk environment or whether additional audit or review is required for the bank to properly assess the third party's control environment.

[14] https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-21.html