Association for Financial Markets in Europe

Consultation Response

PRA CP30/19 Outsourcing and Third Party Risk Management

1 October 2020

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on **PRA CP30/19 OUTSOURCING AND THIRD PARTY RISK MANAGEMENT**. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

Executive Summary

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to respond to the PRA's Consultation Paper 30/19 ("CP"), which include a draft Supervisory Statement ("SS"), on proposals for outsourcing and third-party risk management.

We welcome the draft SS in providing clarification of how the PRA expects UK banks to approach the EBA Guidelines on Outsourcing Arrangements ("EBA GLs")[1] that were published in February 2019. AFME responded to the EBA GLs consultation in September 2018[2]. We also acknowledge the importance of this draft SS in complimenting the consultation papers on '*Operational resilience: Impact tolerances for important business services*'; issued by the PRA (CP29/19) and FCA (CP19/32). A separate response to CP29/19 and CP19/32 has been submitted by AFME as part of the Global Financial Market Association (GFMA) and in partnership with the International Institute for Finance (IIF). We have included in our response below (*1. Introduction*) comments on the alignment of the draft SS to the operational resilience discussion. Further, we would welcome any commentary from the PRA on the expected alignment with future measures proposed from the European Commission, in particular the digital operational resilience act (DORA)[3] and the supervisory oversight of critical third parties and measures to address any potential concentration risk.

Finally. we welcome the PRA draft SS as a mechanism for supporting the industry in facilitating increased adoption of cloud and other new technologies. In our AFME 2019 paper, *The Adoption of Public Cloud Computing in Capital Markets*[4], we identified that *"cloud computing is one of the key technologies that has the potential to shape the development of Europe's capital markets in the next five to ten years."*

We have identified the following high-level considerations for the PRA in response to this draft SS:

[1] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements
[2] https://www.afme.eu/portals/0/globalassets/downloads/consultation-responses/afme-prd-eba-draft-outsourcing-guidelines.pdf
[3] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en
[4] https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20Cloud%20Paper%20November%202019%20Final.pdf

Association for Financial Markets in Europe
London Office: 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 788 3971
Frankfurt Office: Bürohaus an der Alten Oper, Neue Mainzer Straße 75, 60311 Frankfurt am Main, Germany
T: +49 (0)69 153 258 967
www.afme.eu

- Timelines: we would welcome confirmation that implementation timelines for this CP and the PRA's work on operational resilience will be harmonised, and that Register implementation will be consulted on and harmonised with the EU27 where possible to reduce complexity for cross-border firms.
- Scope: we suggest below some clarifications that should be made to the definition of outsourcing, and also that the SS's application to third party arrangements should be clearly defined. The application to third party arrangements should also be considered for a longer implementation timeline.
- Proportionality: we would welcome guidance from the PRA on firms' ability to tailor their application of the requirements to the risk profile of the outsourcing/third party arrangement.
- Materiality: we would welcome further discussion with the PRA on how materiality should be assessed, with examples where possible.
- Register: we would appreciate clarity from the PRA that it intends to consult further on its plans for an Outsourcing Register and would welcome further discussions on proportionality in its application.

Our detailed response to this CP is provided below and AFME would welcome the opportunity to discuss with the PRA our response to this CP.

Comments on the PRA's Draft Supervisory Statement (SS)

Overall Comments

We outline below several areas where more clarity from the PRA would be helpful. However, we are also mindful of the need to maintain the PRA's general principles-based approach and to avoid prescriptive granularity. This may unintentionally restrict firm's flexibility to implement the requirements in a proportionate manner. We would be happy to discuss further any potential conflict in this regard.

In relation to the timing of implementation, we note that the CP appears to be forward-looking, capturing *"UK branches of overseas firms"*. However, until the end of the Brexit transition period, UK branches of EEA firms will not be subject to PRA outsourcing rules. We would request that the applicability of the SS is clarified to expressly exclude EEA firms, and UK branches of EEA firms for the duration of the Brexit transition period. As the SS will ultimately apply to such branches, given the PRA's current approach to branches of third country firms, we would request that additional time is given to such branches, given the PRA requirements under the SS set a different standard to those contained in the EBA GLs (in terms of applicability to arrangements and scope of requirements). We note that consultation papers from other regulators (such as the FCA) have sought to make the distinction between the pre-and post-Brexit transition period as regards applicability, and query whether this approach would be suitable here.

Finally, we note that the use of cloud has been particularly important for firms during the disruption caused by COVID-19. Firms' operational resilience has been boosted by cloud features such as: the geographical distribution of data centres across zones and regions; cloud redundancy allowing multiple copies of data, systems and equipment across regions and thereby ensuring continuity of service in the event of unexpected failures; elasticity which has be crucial in meeting unprecedented peak demands during the pandemic; and the focus of cloud service providers on having highly resilient infrastructures. We believe that this should support the statement in paragraph 1.9 in relation to "enhanced resilience compared to firms' on-premise data centres" – it is reasonable to assume that, had firms exclusively relied on their own physical data centres (and not outsourced some of our data and systems to Cloud), they may have faced greater operational vulnerabilities in these stressed conditions.

1. Introduction (pages 19 – 22)

The PRA is consulting separately on new rules on operational resilience in CP29/19, which has been published simultaneously with this CP. AFME, as part of the GFMA and in partnership with the IIF, has provided a separate response to CP29/19. CP29/19 is proposing to apply the requirements in the Operational Resilience Parts of the PRA Rulebook and the Operational Resilience Chapter in the Group Supervision Part of the Rulebook to all arrangements between firms and third parties. This will include draft Rule 4.1, which would require firms to identify and document *"the necessary people, processes, technology, facilities and information required to deliver each of its important business services"*.

The application of this rule to all arrangements between firms and third parties, for the delivery of important business services, could be potentially difficult to execute in practice. For example, certain third parties consider some of the information required for 'mapping' as confidential, (e.g. the exact number of FTEs supporting a service). This would make complying with requirements under draft Rule 4.1 difficult and could impact the ability to define and test impact tolerances where this third party information and/or involvement is required.

The PRA should consider a more outcome driven approach, where firms can demonstrate meeting the expected outcomes of operational resiliency requirements, in the case of arrangements between firms and third parties.

We would urge the PRA to ensure alignment across outsourcing and operational resilience rules. Clarity on stress testing requirements within a firm and within a sectoral context would also be useful to align approaches across regulations, as well as on expectations when outsourcing to a non-regulated third party that is not bound to the same standards that a regulated firm is.

Finally, we would welcome clarity on the PRA's implementation timeline, given the strong linkages between this CP and the PRA's Operational Resilience work, which is also under consultation. A phased timeline would be helpful for firms in order to take into account the relevant dependencies. The two workstreams have the greatest potential benefits when delivered in tandem and the industry is keen to ensure that this underpins their implementation of each.

2. Definitions and Scope (pages 23 – 24)

Third Party Arrangements:

The PRA Rulebook defines outsourcing as: *"an arrangement of any form between a customer and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub outsourcing, which would otherwise be undertaken by the firm itself"*[5]. Further, Paragraph 2.6 in the CP proposes firms to "assume that activities, functions, services performed or provided by third parties in a *"prudential context"*, as defined in the PRA Rulebook, fall within the definition of 'outsourcing'."

This additional layer to the definition of outsourcing within the draft Supervisory Statement, and its reference to *"prudential context"*, has raised questions within the industry as to whether activities such as Custody services, Depositary services, and Collateral Management services, would fall within the PRA's proposed definition of *"outsourcing"*. AFME's view is that traditionally these services have not fallen into the definition of outsourcing as outsourcing is linked to the concept that a firm is engaging a third party to do something that it could have done itself. Although AFME's view is that it is not practically possible for a firm to provide these services themselves across multiple markets, and we are of the view that these services fall outside the

[5] http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/53220/27-01-2020

definition of *"prudential context"*, AFME recommends that the PRA expressly rules Custody services, Depositary services and Collateral Management services out of scope of the PRA's Supervisory Statement

Furthermore, activities associated with Custody services, Depositary services and Collateral Management services are regulated through multiple rules and requirements within the UK regulatory framework. For example, the rules set out in the UK's Client Assets Sourcebook (CASS), the Alternative Investment Fund Managers Directive (AIFMD), Undertakings for the Collective Investment in Transferable Securities (UCITS), Central Securities Depositories Regulation (CSDR), European Market Infrastructure Regulation (EMIR), Operational Continuity In Resolution (OCIR) and, in the future, the proposed new operational resilience framework which is currently being consulted on in the UK. By including activity associated with Custody services, Depositary services and Collateral Management services within the definitions of outsourcing, this would add additional regulation to address risks that are already appropriately addressed through current regulations.

We are therefore concerned by the assertion in paragraph 2.4 that "*all activities, functions and services performed or provided by third parties in a 'prudential context'…should come under the definition of outsourcing"*. While we note the PRA's overall message that the substance of an arrangement is key, rather than the name it is given, we suggest that these services should fall under third party risk management, but not automatically outsourcing, given the different expectations with regards to each. We are happy to further discuss the details of the current UK regulatory framework and how this applies to activities associated Custody services, Depositary services and Collateral Management services.

In relation to *"the purchase of certain of software products or technology solutions"* under paragraph 2.6, we are concerned by the wide scope and request for additional clarity as to what is intended to be captured. In this respect, we reference our arguments below in respect of the need for a materiality threshold to be applied to these arrangements. Additionally, greater clarity is requested in relation to *"the sharing of data with third parties"* and whether this is intended to refer to all types of data or only specific types.

Under paragraph 2.7, AFME is of the view that firms should have third-party risk management frameworks with *some* of the components highlighted in the draft in respect of Outsourcing arrangements. However, the full components applicable to outsourcing are not necessary for all third-party arrangements. We would be grateful if the PRA could confirm this interpretation.

Additionally, does a third-party *"arrangement"* refer to a group of services or a single service?

Finally, we suggest that, given the expanded scope in relation to third parties and the considerable number of arrangements this will encompass for each firm, additional implementation time is granted for these arrangements.

Ongoing Basis:

Furthermore, while the proposed definition of outsourcing largely mirrors the approach of the EBA, we note that the EBAs GLs provide further clarification that a service should be provided on a 'recurring or ongoing' basis. Specifically, the EBA GLs note in paragraph 26 that:

> *Within this assessment [of whether the arrangement is considered outsourcing], consideration should be given to whether the function (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider and whether this function (or part thereof) would normally fall within the scope of functions that would or could realistically be performed by institutions or payment institutions, even if the institution or payment institution has not performed this function in the past itself*.

A similar clarification is not provided by the PRA. Therefore, under the current PRA draft Supervisory Statement, a one-off or single service could be subject to the strict requirements on outsourcing. However,

such non-ongoing services can have a significantly reduced risk profile and do not require ongoing management as does a recurring arrangement. Therefore, we request the addition of the text set out above, as the current drafting of the supervisory statement appears overly broad. In addition, we suggest that the same criterion is applied to the PRA's definition of material third parties.

Other Comments:

The definitions of cloud services in the EBA GLs are considered useful by firms and we request that these are repeated in the PRA's own requirements.

The Final Report on the EBA GLs confirmed on page 81 that intra-entity arrangements (i.e. head office-to-branch or branch-to-branch) are not outsourcing. It would be helpful if the PRA could make a similar clarification that these are not to be considered outsourcing or, where applicable, sub-outsourcing. We understand that one of the purposes of the SS is to implement the EBA GLs, and that in some areas the PRA wishes to add further clarity/detail, but whilst also seeking to avoid adding new substantive requirements. We do feel though that on this specific intra-entity issue, the PRA's position is in conflict with the EBA and this area should be subject to further consideration. We consider that the conflicting positions taken by the regulators are likely to create difficulties within EEA banks in particular, e.g. an arrangement between a head office in the EEA and a UK branch would not need to comply with the EBA GLs, but it would need to comply with the SS.

If the PRA is steadfast in its view that intra-entity arrangements should be classified as outsourcing, then for UK branches currently seeking 'third country branch' authorisation (who do not currently need to comply with PRA outsourcing rules), we would request that additional time is given to such branches to comply with requirements in this area given the PRA differs from the EBA position. We would also request that the PRA provides further guidance regarding the concept of "proportionality" in the context of this issue. Please see the next section below for further detail here.

We also suggest that clarity is provided, mirroring the EBA GLs paragraph 28, as to which activities should not be considered under the outsourcing definition.

3. Proportionality (pages 25 – 27)

Intra-Group Arrangements:

While we understand that intra-group outsourcing is not inherently less risky, we strongly support the statements in 3.3 – 3.8 made by the PRA in relation to proportionality. Firms should be able to place reliance on their existing policies and processes to address certain outsourcing requirements; in the context of intra-group and avoid duplicating them under the firm's outsourcing program. For example, exit planning should be addressed as part of local and firm wide business continuity planning.

As regards intra-entity arrangements specifically, we would request that the PRA provides further guidance regarding the concept of "proportionality" to give banks' greater discretion as to how they can comply with the SS. We request that the need to comply with requirements under the SS would not be as stringent in this context, and that banks could apply proportionality using an outcomes-focused solution (e.g. considering arrangements from an operational resilience perspective to ensure material services are resilient, rather than implementing all the requirements in the SS). This approach should also take into consideration the location of the two parts of the entity involved, i.e. UK branch to non-UK head office, or non-UK branch to UK head office. We would also request that the concept of "proportionality" is considered in relation to intra-entity sub-outsourcing – please see the relevant section below.

Ring Fencing:

Related to this, clarity would be welcome for those firms subject to the UK's Ring Fencing requirements. This would be in particular for intragroup arrangements that sit within the wider group perimeter, but outside the UK Ring-Fenced group. For example, if a firm has clarity that the provider follows Group policies and Group enterprise-wide risk management frameworks (including 2LOD oversight and 3LOD assurance), and are monitoring service performance and contractual obligations, we suggest that this should be sufficient and that detailed due diligence over the entity (to the same level for an 'external' third-party) should not be required.

Cloud Models:

Finally, we note that the risk profile of different cloud deployments is also important to consider. The presence of cloud as part of an outsourcing arrangement should not act as an automatic indication of risk without an appropriate assessment. For example, a private cloud that is wholly owned and managed within a corporate group is much closer to traditional on-premises models of IT provision than some other uses of cloud. Under certain arrangements, the cloud infrastructure could be owned, operated and provisioned for exclusive use by a single corporate group. As such the firm would have enhanced oversight of, and input into the design of, the mitigating controls put in place. As a result, such outsourcing engagements (e.g. engagements that are supported by applications/systems that are hosted on a private cloud or data that is processed via a private cloud) should not be automatically perceived as more susceptible to risk than that provisioned through traditional hardware model.

Similarly, certain cloud-hosted applications or tools used industry-wide as required, using non-material data (e.g. HMRC web-enabled tax tools, web-based user productivity tools), should not be subject to such strict governance requirements as more comprehensive cloud-hosted applications or services. Proportionality of application, linked to both the cloud model and the underlying service, would be welcomed.

4. Governance and Record-keeping (pages 28 – 31)

Governance:

A firm's outsourcing policy should be reflective of the risk appetite as set by the Board, be reviewed and approved through an internal governance framework, and be validated through the firm's internal control environment. In respect of multi-national groups, AFME asks the PRA to take into account that firm wide outsourcing polices will be promulgated by relevant group-wide functions.

In relation to paragraph 4.4, we suggest that *"reliance on critical service providers"* should refer only outsourcing to and not to third parties.

Under paragraph 4.8, we understand that the PRA expects that overall accountability for Outsourcing and Third-Party Risk Management to the Board would sit with SMF24. However, we request further clarity that sub-accountabilities may be shared across other SMFs based on their respective obligations. For example, whilst Information Security and Resilience will typically also sit under SMF24, other risk-types (e.g. Data Protection, Financial Crime, etc.) will sit under other SMFs. Further clarity on the obligations of the SMF24 versus other key SMFs will assist in clarifying accountabilities and enable more effective embedding across firms. Typically, each third-party arrangement is owned by a specific business line and accountable Executive. As such, it is also important that we do not dilute this risk ownership.

Outsourcing Register:

AFME welcomes all efforts leading to standardisation of regulatory requirements and supervisory practices across multiple jurisdictions, including a common format for an Outsourcing Register ("Register"). We request that the PRA ensures that any further clarifications on the format or the content of the Register does not create

discrepancies across other jurisdictions where the Register format proposed under the EBA Guidelines on Outsourcing is required. To the extent that PRA were to include local discrepancies, if deemed necessary, we recommend that the layout of the Register is maintained and that the local overlay is created in a separate additional section. This would assist with consistency across European jurisdictions. As cross-border firms, AFME's members will need to ensure that their implementation of Register requirements is compliant across all relevant jurisdictions, which will also increase their overall implementation timelines.

In relation to intra-group outsourcing arrangements, we request that the PRA considers whether the Register requirements could be refined. For example, whilst firms will maintain details of intra-group outsourcing, proportionality could be applied to non-material intra-group outsourcing arrangements.

We also suggest that the format and content of the Register are not mandated within the rules themselves, as this is likely to limit the ability of the PRA to adapt the requirements over time to emerging risks and focus areas.

We understand that the PRA would welcome views on the Register and the proposal for an online portal, including the potential practicalities and timeline for development and implementation. In principle, we are supportive of this proposal, provided that appropriate consultation on the design, format and governance of the Register is undertaken. Specifically, we emphasise that any movement of outstanding information onto an online portal would need to be carefully considered from a security and vulnerability perspective, noting that the information stored on the online portal is likely to be highly confidential and/or commercially sensitive. From a practical perspective, this would likely take some time for firms to implement, and we would recommend that the PRA undertake a separate consultation that is dedicated to this topic, to include governance, jurisdictional scope and funding, as well as whether use of the portal would be mandatory. From a timing perspective we would suggest that this consultation process commences in Q1 2022, after the EBA GL compliance deadline of December 2021.

We note that the PRA seeks views on broadening the Register to include third party arrangements outlined in paragraphs 2.5 and 2.6. We suggest that consideration is given to the scale of such an extension, particularly in relation to the number of additional data points this would include. We suggest that needing to document such arrangements should be limited to instances where there is risk associated with the arrangement that would be necessary for the PRA to have oversight. It would therefore be appropriate to apply materiality criteria to prevent against overly burdensome record keeping requirements, that do not provide a benefit to the PRA, and is commensurate with the reporting cost associated for firms.

Finally, we request clarity as to how different sub-outsourcing arrangements, particularly those involving group entities, should be reflected in the Register.

5. Pre-outsourcing Phase (pages 32 – 36)

Materiality Assessments:

In relation to materiality assessments, we suggest that further discussion on the PRA's expectations would be helpful. For example, in relation to 'scaling up' the use of a service under paragraph 5.6: as the PRA acknowledges, materiality may vary throughout the duration of an agreement. Therefore, not all changes in scale may be significant. In this respect, AFME recommends that the PRA acknowledge that the assessment of materiality in the context 'scaling up' should only be in reference to instances where there is material change in the underlying service provided or its associated risk. 'Scaling up' a service in the context of an existing contractual arrangement should not be included, noting that the relevant due diligence and materiality assessment would have already been undertaken with reference to the service parameters in the existing contract. Similarly, an organisational change at a service provider or material sub-outsourced services provider may also not be significant, as it would not change the materiality of the outsourced service. Some

specific scenarios of what would or would not be considered material outsourcing would be helpful from the PRA, particularly in relation to the use of cloud services (which we discuss further below).

We support the statement in paragraph 5.8 that firms should develop their own processes for materiality assessments, considering the criteria listed in the draft SS and in conjunction with their supervisors. This may naturally result in firms taking different views on outsourcing services which may seem similar, which should therefore be recognised as an acceptable outcome.

We would also welcome clarity that materiality assessments may be performed at the service agreement level, rather than at an arrangement level. This is because firms often outsource several different services/processes under one arrangement. These services/processes may have very different levels of materiality. We note that the Register is completed at service level.

Furthermore, we note that in paragraph 5.9, the PRA have indicated that *"a firm should generally consider an outsourcing arrangement as material where a defect or failure in its performance could materially impair the firms 'requirements under 'relevant legislation'"*[6]. The equivalent language in the EBA Guidelines states that institutions should consider a function as critical or important where a defect or failure in its performance would materially impair its "*continuing compliance with the conditions of [its] authorisation or its other obligations under Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive 2014/65/EU, Directive (EU) 2015/2366 and Directive 2009/110/EC and their regulatory obligations*". AFME is of the view that the use of 'relevant legislation' by the PRA has expanded the materiality assessment to include an assessment of compliance with any enactment and any applicable EU regulation. The EBA approach is limited to an assessment of compliance with regulatory obligations under MiFID (i.e. national legislation implementing that). AFME therefore recommends that the PRA aligns its language with the EBA.

Further, the PRA have also set out that an outsourcing arrangement is material where a defect or failure in its performance could materially impact the firms' "safety and soundness" and *"OCIR and resolvability"*.[7] AFME is of the view that these factors both fall within the 'soundness or continuity' text of the EBA Outsourcing Guidelines.[8] We suggest that *"OCIR and resolvability"* is removed and also request clarification that the PRA does not intend to expand on the EBA approach.

There is also no common view on what constitutes *"material"* in relation to cloud and it would be useful for firms to know how the materiality assessment is undertaken in relation to different cloud models. There are different service models and architecture that should be part of the assessment of materiality, combined with the business use. It would be useful for firms to have guidance on the integral part of the materiality decision in relation to cloud (for example, whether the application or activity undertaken in the cloud, the data on the application, or the adopted service model). AFME emphasises the comments made above, noting that in the outsourcing engagements that have a cloud attribute should not be automatically assessed as material unless materiality criteria are met.

Given the PRA's amended definition of *"material"* outsourcing, we request clarity as to how the PRA will expect firms to notify if any existing outsourcing arrangements will be newly classed as material following the publication of the final SS.

Notifications:

The draft SS notes under 5.13 that firms may be required to submit additional information to the PRA following their notification of a new or amended outsourcing arrangement. Whilst AFME's members appreciate the importance of this provision, particular in relation to large or systemically important firms, it

[6] Defined as FSMA; the Capital Requirements Regulations (CRR); the Solvency 2 Regulations 2015; any other enactment; or any directly applicable EU regulation http://www.prarulebook.co.uk/rulebook/Content/Part/211407/26-06-2019

[7] See 5.9 of the draft PRA Supervisory Statement.

[8] 'the soundness or continuity of their banking and payment services and activities' as per paragraph 29(a)(iii) of the EBA Guidelines on outsourcing arrangements. https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

would be helpful if the PRA could consider providing further guidance in this regard. For example, guidance for firms' compliance functions on what information the PRA may expect to be presented as part of an initial request. This would assist in engaging the right stakeholders across a firm and prevent unnecessary delays in progressing outsourcing arrangements.

Due Diligence:

It would be helpful to clarify, in relation to paragraphs 5.15-5.18, whether the PRA has separate expectations for due diligence in relation to prospective/planned providers versus existing providers.

Responsibility for Assessing Concentration Risk:

In relation to concentration risk under 5.21, further dialogue is requested as to how the PRA intends to address industry-wide concentration risk, given the current lack of industry-wide criteria to determine this. For example, firms already perform risk analysis of their concentration within individual cloud providers across their businesses, which must be done at a granular level both to ensure it captures the level and criticality of each outsourcing arrangement, and to take into account the service offering and resilience of each cloud provider. Firms also perform analysis of the cloud dependencies of their supply chains.

However, it is supervisors, such as the PRA, who can take a view of concentration risk across the industry to determine systemic risk. For risks of this nature, supervisors are well positioned to have oversight at an industry level, as compared to FIs individually. It would be helpful to discuss further with the PRA how data provided by firms can assist with this analysis and how the PRA intends to address systemic concentration risks against, for example, the increased resilience and security offered by outsourced services such as cloud. We believe that further regulation specific to management of third-party providers in financial services as a means to reduce or eliminate concentration risk is not an optimal solution. Therefore, as we note below, the focus should be on reducing the risks arising from concentration through existing tools and stronger resiliency planning.

AFME would appreciate the opportunity to continue working with the PRA in its efforts to address concentration risk as part of this CP.

Further Comments on Concentration Risk:

We believe that any assessment of concentration risk should not restrict the choice of outsourcing arrangements or providers available to firms. The focus should be on reducing the risks arising from concentration rather than reducing concentration itself. Similarly, we support the efforts by UK and other authorities to encourage greater use of technologies such as cloud computing, which itself requires ensuring the optimal environment for greater competition rather than restricting third party provider choice.

We request that the PRA provides further detail as to what it considers to be *"closely connected service providers"* under paragraph 5.21. For example, we suggest that it should mean *"service providers with legal entities rolling up to the same parent entity"*.

Furthermore, the CP states in paragraph 2.48 that *"A single service provider, or a small number of service providers which are very difficult to substitute may, in some cases, dominate the provision of certain outsourced and third party services to large numbers of PRA-regulated firms (hereafter 'systemic third parties')."* On this point, the FCA Handbook, SYSC 13.9.4(5) states, *"Before entering into, or significantly changing, an outsourcing arrangement, a firm should: consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several firms."* While we understand the risk of failure of a single service provider used by several firms, it is generally not possible for firms to ascertain the extent to which other firms are using the same service provider (for example, due to confidentiality provisions in their contracts). This would only be visible to supervisory authorities. However, we agree that concentration with single service providers should be regularly monitored and reduced or mitigated in

instances where a vulnerability is detected, for example through Business Continuity Management plans that are regularly tested.

Finally, we note that other areas of the industry exist where concentration within a few providers is accepted and managed, such as central clearing. We suggest that consideration is given to how such models can exist without posing unacceptable risk levels. The lessons learned from such models may be able to be applied at this early stage to other outsourced service providers where firms are not yet critically dependent.

6. Outsourcing Agreements (pages 37 – 38)

In relation to this section, where the language used by the PRA differs from that used in the EBA GLs, we request that the language is aligned. Where it cannot be, we request clarity as to why it differs and where PRA requirements should take precedence over the EBA GLs.

In relation to paragraph 6.5, we request that the PRA provides some examples of relevant *"support services"*. We also note that, for intragroup outsourcing, *"renewal date"* and *"end date"* may not be applicable and should not be required.

The right of firms to monitor a service against specific key performance indicators (KPIs) may not be expressly indicated in a service provider's contract. Additionally, these are not necessarily the metrics by which a firm monitors and manages outsourcing arrangements – instead firms may use other methods which are not KPIs in a legal sense, for example: benchmarking, customer satisfaction surveys, attrition of key personnel, or acceptance testing. We therefore suggest that monitoring against KPIs is given as an example, not a requirement.

In relation to two of the items under 6.5, *"the requirements for both parties to implement and test business contingency plans"* and that *"both parties should commit to take reasonable steps to support the testing of firms' termination plans"*, we suggest that it is not appropriate for the requirement upon outsourcing firms in each case to be documented in the Outsourcing Agreement. While the service provider obligations should be documented here, the requirements upon the firm would better sit elsewhere in the SS.

We note the requirements under 4.11 for firms to make service providers aware of internal policies and under 8.1 of regulatory powers and requirements. We request the PRA confirm that it is sufficient to achieve this via an outsourcing agreement, where this is acknowledged by the service provider in signing the agreement and the terms contained within.

Finally, we suggest that Sections 7, 8, 9 and 10 of the draft SS should be captured in outsourcing agreements only at a general level, given that the details will be subject to change (for example, use of confidential data). Instead this level of detail should be held elsewhere as part of an overall third-party risk management framework and there should be recognition the details may be part of relevant intra-group policies or standards in the context of intra-group arrangements..

7. Data Security (pages 39 – 41)

Shared Responsibility Model:

The concept of a *"shared responsibility model"*, outlined in paragraphs 7.2 and 7.3 in relation to data security, whilst common in the industry, is an addition to the requirements set out in the EBA GLs. As such, it would be helpful to discuss further with the PRA the broad expectations on firms in this regard, and in particular the expectations on the service provider.

In addition to considering firms' obligations within the shared responsibility model, we believe there is potentially an important role for regulators in determining how to extend the umbrella of financial regulation

to cloud service providers who handle financial data. Such a focus would ensure that the incentives between financial institutions and third-party service providers, such as cloud providers, are appropriately aligned.

Other Comments:

We suggest that the PRA remove *"data location"* from the *"data security"* section. Whilst physical location of data may be important from a Business Continuity Planning (BCP) and resilience perspective, it is does not have an impact on technical security (consideration of the political and legal regime under which the service is provided and data stored should be separate from security). Including "data location" could also inadvertently support greater data localisation within the industry, which can detract from security, inhibit innovation, and impose unnecessary costs.

In relation to Table 5, Software as a Service (SaaS) providers are required to have appropriate written agreements with their sub-contractors, including with respect to data. We request that the PRA confirm that these clauses are sufficient.

It would be helpful for the language in paragraphs 7.8 and 7.10 to be amended for consistency (i.e. data-at-rest/data-at-use/data-in-transit/data-in-memory).

We suggest that the list of controls for data security in paragraph 7.10 may be overly prescriptive to apply to every scenario. It may not be necessary to include all these controls in every contract. For example, in a SaaS environment, encrypting data in memory is a difficult control for firms to implement while there other controls that can seek to maintain confidentiality for data in memory in SaaS environments more efficiently. Alternatively, the data stored may be publicly available information making encryption significantly disproportionate to the risk of unauthorised access. Instead, we propose that the drafting is amended to *"these controls…may in include, but are not necessarily limited to…"*, in order to provide firms with greater flexibility to apply controls based on risk.

The PRA also proposes that where encrypted data is used, the firm will need to provide an accessible encryption key for the PRA, so that it is secure and accessible (in accordance with Fundamental Rule 7). Fundamental Rule 7 states:

> *"A firm must deal with its regulators in an open and co-operative way, and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice."*

We strongly suggest that this should be a reactive obligation on a firm, so that the regulator can access the information as and when needed. As such, we suggest that firms provide decrypted data on a need to know basis, as opposed to a blanket requirement to provide the information in any instance. Provision of encryption key information would require extremely strict security and controls given its highly sensitive nature, and would likely still pose an unacceptable information security risk to firms.

8. Access, Audit and Information Rights (pages 42 – 45)

In relation to paragraph 8.4, that security penetration testing should be carried out *"where relevant"*, we suggest that it is likely to be difficult to impose the requirement to test an outsourcing provider in this way due to their own security procedures. It is more likely that an outsourcing provider could agree to provide the firm with its own penetration testing results, where relevant, or provide the results of third party testing. It would be helpful if the PRA could support the industry in moving towards such a model, particularly where related to cybersecurity audits or the audit of an industry utility. We also suggest that an alternative solution on testing could be for large service providers to share audit reports with the PRA, which could then be shared with regulated entities as applicable. Shared assessments, or a utility-style model, would also benefit service providers who would not be faced with multiple requests from their users.

9. Sub-outsourcing (pages 46 – 47)

Outsourcing Chains:

We request that the requirements on firms for sub-outsourcing are applied in a proportionate manner, noting that it will be difficult for firms to monitor all the parties in an outsourcing chain. For example, agreements can document the obligations on the third party to their sub-service providers, but firms will be reliant on the third party for monitoring against impact tolerances and for disclosure of due diligence and risk assessments (clarity regarding the PRA's expectations on timings for compliance with this obligation would be welcomed).

It would be helpful if the PRA could provide clarity that the identification, assessment, management, and reporting of fourth-party risks should be focused on sub-contracting / sub-outsourcing of 'material outsourcing' arrangements only, and that firms are only required to understand sub-contracting / sub-outsourcing by the third-party, rather than broader critical fourth-parties that are not sub-outsourced / contracted.

In addition, firms would welcome confirmation that this approach is consistent with the principles of the Operational Resilience CP, whereby understanding the impacts on an important business service is not limited to just 'critical outsourcing' arrangements, of the sub-outsourcing / sub-contracting components of these arrangements.

Given the challenge to firms of implementing a robust and effective third party risk management framework, we do not believe it is realistic to extend beyond fourth-parties (e.g. 5th parties, 6th parties, …, Nth parties). We would propose that focus should be on obtaining assurance that 'material outsourced' providers have robust third-party risk and supply chain frameworks, procedures to ensure contractual flow-down to their own supply chain, and procedures to monitor and assure their own supply chain (where critical). We would also welcome the PRA in recognising that this will be easier with certain providers depending on their market position.

We also would like to request the PRA provide further examples of approaches that would be considered acceptable under the sub-outsourcing arrangements, for example:

- identifying and periodically reviewing a set of scenarios, and;
- mapping the risk assessment process steps against these scenarios to ensure full coverage.

SaaS:

In the context of SaaS, we believe that all components of that service are a single outsourcing arrangement if provided by the same provider. For instance, if the provider of the software also hosts on their own infrastructure, the infrastructure hosting is not considered sub-outsourcing.

Intra-group Arrangements:

From an intra-entity perspective, we query whether a UK branch is expected to have oversight of all relevant material sub-outsourcing by its head office (for example) to all other branches in the Group (i.e. all the arrangements are still provided within the same legal entity), ensure compliance in such sub-outsourcing agreements, and record such sub-outsourcings in the UK branch's register? This would feel like an overly burdensome obligation considering the head office is responsible for such sub-outsourcing, and we would request that the concept of "proportionality" addresses this issue to lessen the compliance burden on banks in this area (e.g., by allowing UK branches to rely on their own branch-level control framework from an operational resilience perspective, rather than being required to comply with these requirements). We further request that additional time is given to UK branches of EEA banks to comply with these requirements in the

event that the PRA does insist on some degree of oversight by the UK branch of its EEA head office's intra-entity sub-outsourcing arrangements.

Our comments are similar in relation to intra-group sub-outsourcing arrangements (where we acknowledge that the sub-outsourcing by head office is with a different legal entity), but there should still be some degree of flexibility for banks from a proportionality perspective as the EEA head office is still ultimately responsible for the sub-outsourcing.

10. Business Continuity and Exit Plans (pages 48 – 51)

The draft SS refers to both *"exit plans"* and *"exit strategies"* – we request clarification as to whether these are intended to refer to the same concern. It is our understanding that firms would generally understand these as separate concepts. For example, an exit plan documents end-to-end transitions and places specific obligations on the outsourcing provider to co-operate fully both with the firm and any new outsource provider, including removing data from the previous service provider's systems on exit. On the other hand, exit strategies ensure that plans are in place and fully tested.

The draft SS proposes to include expectations on the governance of business continuity and exit plans, for instance, for firms to develop plans during the pre-outsourcing phase. AFME acknowledges the need for an effective exit plan for material outsourcing and that potential exit strategies would be taken into account as part of the decision to outsource.

However, development of a comprehensive and granular exit plan at the pre-outsourcing stage is generally not feasible at this stage in the outsourcing process, as a firm has yet to execute the arrangement and is unlikely to be fully aware of how the service provider would structure the service offering. A firm's exit plan is likely to be further refined throughout the outsourcing decision process. A suggested approach would be to allow firms to create an overall exit plan as part of the decision to outsource and then develop the granular details during a set period following the go-live of the service.

We also suggest that the level of exit and contingency planning required will need to be tailored to the specific outsourcing arrangement, e.g. intra-group outsourcing vs an external provider. Furthermore, where multiple services are outsourced to the same provider, the exit or contingency plan may be most appropriate at an overall level rather than having individual plans for each service.

In relation to paragraph 10.5 on cloud outsourcing arrangements, clarity is requested as to how *"multiple availability zones"* should be understood.

Appendix: Guidance for Completing the Outsourcing Register (pages 52 – 54)

It would be helpful for firms if the PRA were able to provide an early indication of what taxonomies are envisaged for the submission of inventories e.g. vendor name, legal entity identifiers, service category/departments, organisational structure.

AFME contacts

David Ostojitsch, david.ostojitsch@afme.eu +44 (0)20 3828 2761
Fiona Willis, fiona.willis@afme.eu +44 (0)20 3828 2739