UK Finance
5th Floor
1 Angel Court
London
EC2R 7HJ

Orlando Fernández
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA

30 September 2020

UK Finance response to PRA Consultation Paper on Outsourcing and third party risk management (CP30/19)

1. About us

UK Finance is the collective voice for the banking and finance sector. Representing more than 250 firms, we act to enhance competitiveness, support customers, and facilitate innovation.

2. Executive Summary

On behalf of our members, we welcome the opportunity to comment on the Prudential Regulation Authority's (PRA) draft Supervisory Statement (S/S). Since the publication of the European Banking Authority's (EBA) Guidelines on outsourcing arrangements (EBA GLs) we have been engaged with members, providing them with forums to discuss this topic and the practical considerations of implementing what is set out in the S/S.

Furthermore, the efforts that the PRA make to be principles based, rather than prescriptive, while focussing on pragmatism and flexibility are extremely important to our members, who are a broad range of firms and as a result may apply differing approaches given their specific circumstances.

For implementation to be effective, members believe that the S/S needs to be tied in to work already ongoing in operational resilience – led by CP29/19 in the UK, and by the Basel Committee on Banking Supervision (BCBS) internationally – and to acknowledge the EBA Guidelines on ICT and security risk management. A continuation of industry engagement by the PRA, which has been well received by members, and a pragmatic approach to supervision would support this approach to delivery and allow our members' focus to be on efficient and effective implementation and optimisation of risk management.

We wish to highlight the following high-level areas that are discussed in more detail in our response:

- EBA GLs – There is concern that the S/S adds additional requirements to the EBA GLs and that there should be closer alignment between the two.
- Proportionality – Further guidance is sought on members ability to tailor their application of the requirements in the S/S to the risk profile of the outsourced or third party supplier. This is particularly pertinent to our non-category 1 members.
- Definitions – Additional clarification, with examples where practical, would be welcomed on how materiality will be assessed, and for outsourcing and sub-outsourcing.
- Outsourcing Register – We request that the PRA consults with industry on its plans for an Outsourcing Register and considers how the implications for firms that have to complete registers in other jurisdictions.

Finally, our members note the number of third-party/outsourcing requirements and expectations on outsourcing that they are subject to in different jurisdictions (with UK and EU obligations listed on page 21 of the CP). Our members request that the PRA remain flexible so that firms are able to adapt their compliance and risk management to account for the different requirements in different jurisdictions. We further request the PRA, wherever possible, avoid prescriptive rules and continue to focus on high-level outcomes and capabilities that they wish firms to possess so that firms can evidence these in the variety of ways that will be necessary for different regulators.

3. Non-Category 1 Firms

The significance of the requirements in the S/S and the operational resilience consultation paper (CP) on non-category 1 firms cannot be overstated but might, due to lack of engagement or visibility, be somewhat overlooked. Those firms may be small or mid-tier institutions based solely in the UK, or foreign branches that are tied into group dependencies for services such as IT infrastructure, treasury management or other key operational platforms.

It is for this reason that a more proportionate application of the requirements in the S/S would be welcomed for non-category 1 firms. In our view this would still meet its policy aims while making it more workable and imposing less of a burden on those firms, given, by definition, the threat posed to the integrity of the financial system of a category 1 versus a non-category 1 firm is materially different.

This proportionate approach could be founded in the firm making well governed risk-based trade-offs between the need for day to day resilience, long term commercial viability and the risks associated with using large technology providers (difficulty of exit, lack of audit information etc.)

Such providers present a different set of challenges to non-category 1 firms. They have a largely inflexible attitude to contractual terms, audit rights, exit provisions and continuity testing, making it difficult for non-category 1 firms to apply the requirements in the S/S. There will also be a knock-on impact to those firms' technology suppliers because most are also dependent on the same large technology suppliers.

The issues with contractual terms, audit rights and exit provisions affect non-category 1 firms more acutely given the difference in commercial power. While we acknowledge that some providers apply a 'take it or leave it' approach no matter what type of firm they are dealing with, the large category 1 firms have considerably more commercial power with suppliers than non-category 1 firms (e.g. mid-sized building societies) and so they have some ability to obtain the necessary provisions from these large technology suppliers.

While the providers present practical difficulties to the application of the S/S and create risks, using them is often an operational and commercial necessity (and indeed desirable) if firms are to maintain the highest levels of operational resilience and continue to be viable financially, as for instance large technology providers are often more capable, flexible and cost effective than in-house options.

4.1 Operational Resilience CP (29/19)

We welcome publication of this CP alongside those on operational resilience (to which we have responded separately), and the seeking of alignment between these two areas. In particular, the operational resilience CPs provide a valuable lens for firms to assess how they should monitor their third parties, fourth parties and beyond, and establish the notion of end-to-end resilience. Our members are supportive of measures that improve operational

resilience, and in this context, it is important to consider whether the outsourcing proposals help to support this.

The view among members is that the operational resilience CP is largely principles-based and gives primacy to firms in making decisions on operational resilience. In contrast, the outsourcing S/S is largely prescriptive, and can be seen to counteract the direction of travel regarding operational resilience.

As an example, the operational resilience CP places the customer at the centre of the UK's resiliency framework. It does this by tasking firms with identifying the most important services that their customers rely on ("important business services"), identifying their vulnerabilities in those services, and then mitigating them. This will require firms to map dependencies, set impact tolerances, and test these parameters through exercising. Because firms must understand what services their customers most rely on, they will have to prioritise their focus to the important services first. This approach will be challenging where firms deploy an operating model across multiple geographies. In contrast, the S/S does not take business services as the starting point. Instead, it starts with "arrangements", which may or may not apply to important business services.

The implications of these requirements are even more pronounced for third country branches, as such branches are more likely to follow 'home state' approaches to requirements on outsourcing, and may even be subject to specific 'home state' regulations on outsourcing, which may conflict with UK host-state regulation. It is important that appropriate deference is given to home state regulators in regard to operational resilience and outsourcing. For global firms, often the best resilience outcomes will come from taking a global approach to resilience management, including on third party dependencies such as outsourcing.

4.2 EBA GLs

Members are of the view that the content of the S/S and the EBA GLs are aligned to some extent. However, there is a view that the S/S diverges from the requirements of the EBA GLs. For example, the S/S extends beyond outsourcing relationships to a wider range of third party (non-outsourcing) relationships. Further, there is an uplift from the EBA GLs for certain requirements, such as, contractual documentation requirements and third-party access/audit rights.

It would be helpful for the PRA to provide further clarification on some definitions and terms. Specifically, with regards to outsourced arrangements members would welcome more clarity on the distinction between a third party arrangement and an outsourcing arrangement to help ensure consistency in the way they are understood across industry.

The S/S at paragraph 1.6 lists 18 regulatory requirements for in-scope financial firms when outsourcing. This is complex and challenging to comply with and members would welcome simplification and streamlining where appropriate, in particular where they are being asked to comply with both the EBA GLs and the S/S which are not identical in certain cases.

Members would welcome clarity that it would be sufficient that in-scope UK financial firms should comply with the wording of the S/S to avoid the application of any conflicting regulations.

Some of our members that have both Banks (falling under the remit of the EBA) and Insurers (falling under the remit of Solvency II/EIOPA) in the same group may at times benefit from the same outsourcing arrangements. Applying multiple regulations, which are contradictory in certain parts, will prove to be easier if the final S/S is presented as a single regulation, which

consists of a harmonised set of principles for outsourcing arrangements that applies to both Banks and Insurers.

Assuming the S/S will apply to UK branches of EEA firms, we would request that additional time for implementation is given to such UK branches, given the PRA requirements under the S/S set a different standard to those contained in the EBA GLs (in terms of applicability to arrangements and scope of requirements).

4.3 Other Guidance

The BCBS has published two consultation documents updating its principles for the management of operational risk (BCBS508) and proposing new principles for operational resilience (BCBS509) to increase the capacity of banks to withstand disruptions due to potentially severe events. The guidance, although high-level, does address outsourcing. It would be helpful for the PRA to explain how it foresees that these and other international requirements will interact with its approaches, particularly given the cross-border nature of some firms' operations and that other jurisdictions are still developing principles in the areas of outsourcing and operational resilience (e.g. the US).

Members generally consider that there have been various regulations and guidance introduced in relation to outsourcing in recent years, some of which firms have not yet had time to implement fully (mainly due to the complexities of installing reforms that are evolving and multi-faceted). In this context, members would appreciate it if the PRA understood this when introducing new requirements over and above these, at least until the other requirements have been installed.

5. Definitions and scope

5.1 Materiality

Our members understand why the term 'material' has been used in the S/S, as opposed to 'critical' or 'important' and support it. However, it is noted that in paragraph 5.9, the use of 'relevant legislation' appears to have expanded the materiality assessment to include an assessment of compliance with any enactment and any applicable EU regulation. The EBA GLs are limited to an assessment of compliance with regulatory obligations under MiFID (i.e. national legislation implementing MiFID). It is therefore recommended that the S/S align its language with the EBA GLs.

Further it is also set out that an outsourcing arrangement is material where a defect or failure in its performance could materially impact the firm's 'safety and soundness' and 'OCIR and resolvability'. Members are of the view that these factors both fall within the 'soundness or continuity' text of the EBA GLs. Clarification that the S/S language does not expand on the EBA GLs would be welcomed.

The Covid-19 pandemic has highlighted that in some scenarios (stress events), some suppliers will become material. Guidance would be welcomed on how to apply the S/S to suppliers that under BAU would not have been deemed material but can become material in certain, exceptional, circumstances. Further, guidance on how a firm would be expected to deal with substitution of a fourth party or nth party supplier under exceptional circumstances.

Clarification is also requested on what would be considered 'material' in the context of cloud, which would provide greater consistency in application across firms, particularly across different cloud models. Members are of the view that when interpreting the S/S and EBA GLs there is an implicit outcome that all cloud should be considered outsourced. However, the

presence of cloud as part of an outsourcing arrangement should not act as an automatic indication of risk or level of materiality without an appropriate assessment of the arrangement.

5.2 Outsourcing

With regards to the definition of 'outsourcing' our members' view is that there continues to be a risk that this is misinterpreted or applied inconsistently by firms. Further examples or clarity would drive greater consistency of application across firms.

In this context, it would be welcomed that the terms 'on-going' or 'recurrent' be included in the S/S. This will help clarify those arrangements that would reasonably be concluded to be outsourced. It is understood through discussions with the PRA that it will change the S/S so that the scope applies to arrangements that are ongoing or recurring (rather than one-off), and members would request that alignment is made with the EBA GLs (section 3, paragraph 26).

The term 'outsourcing' as it relates to services analysed under the EBA GLs may be classified differently to services analysed under the S/S. Our members note that this different definition could give inconsistent results to classified agreements under the EBA GLs. This would result in extensive cost and time to realign to regulatory requirements. It is therefore requested that a more holistic definition of the term 'outsourcing' is provided which aligns more closely to that within the EBA GLs.

5.3 Sub-outsourcing

Members would welcome further clarity on the definition of 'sub-outsourcing', which is not currently included in the S/S. In addition, they would like a distinction to be made between 'sub-outsourcing' and 'sub-contracting', and clarity on what is in and out of scope of these two terms. The prevailing view is that 'sub-outsourcing' requires the transfer of a particular function to a third party, while 'sub-contracting' is the provision of services to support the activities of such functions. Having this interpretation confirmed and clarified in the final S/S would be welcomed.

5.4 Scope

While members recognise the UK authorities' intention to expand their focus beyond outsourcing to third-party risk management more generally, we believe that this represents a significant expansion beyond current best practice. We do not dispute the importance of this shift given changing business models and use of technology, but time must be allowed for firms to embed this expansion into practice and develop new processes for increasing scrutiny of third-parties. We note that this expansion goes beyond the EBA GLs and suggest therefore that the original timelines will need to be reconsidered for this element, as opposed to requirements that were already included in the EBA GLs which remain appropriate.

The assessment of impact 'in a prudential context' (paragraph 2.6) in effect broadens the definition of outsourcing, which in turn could create uncertainty, potential inconsistency of classification and treatment and possibly increase the population of material outsourced arrangements as a consequence.

Paragraph 2.6 proposes firms to "assume that activities, functions and 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 S/S, and its reference to *"prudential context"*, has raised questions amongst members as to whether activities such as custody services, depositary services, and collateral management services, would fall within the PRA's proposed definition of "outsourcing".

The view of our members 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 our members feel that it is not practically possible for a firm to provide these services themselves across multiple markets and are of the view that these services fall outside the definition of "prudential context". Therefore, we recommend that the PRA expressly rules custody services, depositary services and collateral management services out of scope.

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. 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.

Complete clarity is requested on the intended approach and the application of 'in a prudential context' as this could create operational complexity and overlooks the fact that firms may have arrangements classed as non-outsourced, which they treat as high risk and manage accordingly anyway.

There is relatively little guidance specific to branches, other than the statement in paragraph 3.6 that. 'When third-country branches or subsidiaries outsource to parent companies outside the UK, they should ensure that the outsourced service is provided in compliance with UK legal and regulatory requirements.' Further guidance on best practice where a branch is reliant on services that are outsourced at an entity level in particular would be beneficial.

In respect of third parties, under paragraph 2.7, we understand this requires firms to 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.

Lastly, where applications are available for hosting purely on a SaaS basis, as opposed to on premises, it is becoming less clear how these would be viewed as outsourcing purely against the definitions, and additional clarity is request on this point.

6. Proportionality

Members are supportive of paragraphs 3.3 – 3.8 in the S/S and welcome the acknowledgement that 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 programme.

However, they would welcome further clarity on what would constitute a 'reasonable' level of proportionality in an intra-group arrangement. A level of pragmatism would be welcomed around the proportionality that can be applied in terms of how firms meet certain requirements in practice for intra-group arrangements, as opposed to that required of an 'external' provider.

In particular, members feel it is important to recognise that for intra-group outsourcing, control can be exerted outside of a direct ownership structure, for instance between subsidiaries of the same parent where both would have equal influence over a globally applied control set.

As regards intra-entity arrangements specifically, it is requested that the PRA provide further guidance regarding the concept of 'proportionality' to give members greater discretion as to how they can comply with the S/S. In addition, that the need to comply with requirements under the S/S would not be as stringent in this context, and that members 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 S/S). It is also requested that the concept of 'proportionality' is considered in relation to intra-entity sub-outsourcing.

Whilst the intent behind paragraphs 3.7 and 3.8 is welcome, clarification is requested on the applicability of the requirements in the S/S (particularly the relevance of business continuity and/or exit planning requirements) for intra-group outsourcings subject to OCIR and ring-fencing rules.

There appears to be a difference in the approach of the Financial Conduct Authority (FCA) and PRA in respect of intra-group outsourcing, specifically on the principle of proportionality, with the PRA supporting the principle of a proportionate intra-group outsourcing where there is sufficient control over the relevant related firm but the FCA appearing not to endorse the principle of proportionality in this context. Clarification is sought on these approaches and whether this difference is deliberate. To the extent possible, members would welcome consistency between the regulators to avoid the risk of conflicting principles and to assist with implementation of the new requirements.

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 by, and provisioned for, exclusive use of a single corporate group. As such, the firm would have an enhanced ability to exercise oversight and input into the design of the mitigating controls put in place. As a result, such outsourcing arrangements, 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 models.

7. Governance and record-keeping

Members appreciate and understand that the prescribed responsibility for Outsourcing (SMF24) gives clarity for accountability at a board or executive committee level. However, recognition is sought that there can be challenges in ensuring clear accountability for the day-to-day management of outsourcing and third-party risk management below the SMF level.

In particular, a recognition that given the broad spectrum of regulatory requirements, sub-accountabilities may be shared across other SMFs based on their respective obligations. It is requested that timescales for embedding these requirements across often complex firms are realistic and if there are deemed to be circumstances where accountability could be split, these are provided.

7.1 Outsourcing Register

There is consensus among members on the potential challenges of having a consistent data structure, standardising names, and agreeing a consistent taxonomy for the Register, while acknowledging that for members the ability to collate and report this information in a consistent format can prove challenging and is often highly manual. Therefore, an additional consultation specifically focussed on the Register (and an online portal if that is also proposed) is requested.

Based on similar initiatives, some members would find it helpful for the PRA to consider the use of tools or enablers for implementation of such a Register e.g. a data mapping tool. Although there is not consensus agreement on this issue as it will not necessarily be effective given the varying sizes, complexities and business models of other firms.

Regarding a data mapping tool, a centralised mapping of outsourcing will provide significant benefits to firms when planning for operational disruption. The PRA should therefore consider the benefits of mapping the sector and its dependencies to understand systemic operational interdependencies. A central view of dependencies could also allow the PRA and firms to assess the cumulative impact of concentration risk across sectors.

Where the CP invites industry feedback on systemic concentration risks, members believe that this should be done directly by authorities. For risks of this nature, authorities are well positioned to have oversight at an industry level, as compared to individual firms. We believe, however, that any such assessment 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 which we believe would be difficult and require undesirable sacrifices to security, efficiency, and innovation.

For those members that will also have to complete the EBA Register, they wish to minimise (and preferably avoid) discrepancies and duplication of effort in content across jurisdictions. It is requested that the PRA work with other authorities to reduce the need for multiple register requirements which, aside from being an administrative burden, increase the likelihood of data inconsistencies. It is further recommended that if there are local discrepancies, the layout of the EBA Register is maintained and a local overlay is created in a separate additional section.

Establishing the Register is a significant undertaking and will require ongoing management by our members. Ensuring they only collate data points that provide value and will be used by the PRA is key. Our members encourage the PRA to challenge the breadth of data points requested, ensuring that each has value and intended use-case. Understanding the end use of data would assist firms in ensuring they capture the right information.

Further to the above, members would welcome clarity on what is intended to be captured within the Register. For example:

- What is the extent of fourth party data that will be required? Will it be for only those where a material part of a material function has been sub-outsourced?

- Will it be limited to just outsourcing arrangements (both ‘material’ and ‘non-material’ outsourcing) or also broader third-party arrangements, which can cause in some cases a ten-fold difference in volume?

- Where firms use resellers for IT products, for example, will firms be required to include the details of the company that produce / own the product as part of the Register?

- Will the data attributes be exactly the same as the current Outsourcing Register? If there are differences, will the PRA include this in the suggested consultation or provide early visibility of any changes in data attributes to allow these to be captured?

Members are also mindful of the need for the Register, and potentially an online portal, to be designed with security in mind, noting that it will receive highly confidential and/or commercially sensitive data. Consulting with firms on the desired approach will therefore be an important step.

8. Pre-outsourcing phase

Members would find it beneficial if the PRA acknowledged that the assessment of materiality in the context of 'scaling up' (i.e. becoming material following a reassessment) should only be in reference to instances where there is 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.

Members would like it made clear that the criteria in Table 4 of paragraph 5.11 are qualified by materiality of impact. For example, any outsourced arrangement with the personal data of one employee could potentially impact obligations under the General Data Protection Regulation. However, this alone should not be sufficient to classify an outsourcing arrangement as material.

There are also some concerns around the impact of revisiting the critical third parties to address definitions in the EBA GLs and Outsourcing CP. This would impact due-diligence programmes as firms reassess the classification of third parties against the guidance, and BAU third party management, with members finding that their critical third party list has increased significantly.

Clarification is requested within the pre-outsourcing phase on the expectation that the due diligence of fourth parties is now the responsibility of the firm, when the assumption to date has been that third parties could be relied upon for this.

Members welcome the clarity provided on the process that will be put in place for retrospective notification of any agreements that now meet the new definition of material outsourcing or pre-date the requirement for notification. With regards to bulk notification they would prefer to provide this through inclusion of any newly defined material agreements in the Outsourcing Register, while new material outsourced arrangement notifications would follow the standard route via presentation to the PRA.

Where members have indicated that they will update relevant contracts either at renewal or when there is a significant change, they also seek confirmation from the PRA that it is aligning its timescales with the EBA GLs. In the event that the number of outsourcing arrangements increases because of the 'prudential context impact' point (see 3. Definitions and scope), achieving compliance by December 2021 will be operationally difficult for some firms, so a flexible approach to the deadline would be strongly welcomed.

With regards to concentration risk, while this is being considered at a sector level, members' approach to assessing this within their supplier base are at differing levels of maturity. This is a challenging area for our members and a description of the outcome being sought and any examples of best practice would be of assistance.

9. Outsourcing agreements

We are of the view that the remediation of contracts is a significant undertaking and would receive challenge from suppliers. It has notable cost implications and is often more complex than expected. Accordingly, members support alignment of the S/S to the existing EBA GLs.

The timeline for implementation should also consider the design and implementation of the updated operational resilience framework as mandated by the operational resilience CP.

Our members want further clarity around paragraph 6.5 of the S/S in relation to Material Outsourcing Agreements, in particular these sections:

- There is a requirement for 'Court jurisdiction' to be listed in any written agreement. However, there are parties that may elect to use a dispute forum other than courts (e.g. arbitration, expert determination etc.), and hence jurisdictions should not be limited to courts only.

- With regard to differences to the EBA GLs, there is anticipated challenge over termination rights such as those relating to 'impediments capable of altering the performance' (EBA Para 98(b)) or 'weaknesses regarding the management and security of confidential, personal or sensitive data' (EBA Para 98(d)). The S/S does not set out specific scenarios that could give rise to a right to terminate, and therefore the PRA is requested to provide clarification that termination rights should be required for 'material' breach of applicable law, regulations or contractual provisions (including confidentiality and data protection). Members anticipate that some of these changes (e.g. termination rights) will likely increase complexity of negotiations with their suppliers.

- Obtaining buy-in from third parties on 'appropriate corrective action' in the event of service levels not being met can prove challenging, as firms have experienced while implementing the EBA GLs. The PRA is requested to provide more guidance on the corrective actions which they expect.

- Challenge is expected from third parties (including cloud providers) of embedding into contracts the testing of business continuity plans (BCPs), particularly when taking 'account of firms' impact tolerances for important business services. This is compounded by the requirements being pre-outsourcing which means that the firm must be able to identify the impact tolerance for a third party supporting important business services prior to signing the contract. Therefore, there needs to be an understanding that the alignment of timings is important in this respect, particularly where impact tolerances need to be set and agreed.

- Where it is asked that firms apply 'appropriate and proportionate information security related objectives', it should be noted that public cloud providers may not accommodate customer specific security requirements and, in any event, these types of suppliers usually have robust security procedures in place. This situation may also arise with key providers such as financial market infrastructures, trading platforms, exchanges etc. Clarity is sought on whether, in this circumstance, the third-party provider's security policy may be appropriate.

10. Data security

The concept of a 'Shared Responsibility Model', while common in industry, is not outlined in the EBA GLs. As such, members would welcome further clarity on the PRA's expectations in this regard and how this will operate in practice. Specifically, requirements in the EBA GLs which encourage firms to consider the security of the cloud and not only in the cloud, would appear to exceed the standard understanding of the 'shared responsibility model'.

In section 7.6 the PRA requires that firms identify data that "they would need to access and potentially migrate as a matter of priority in the event of a disruption". We disagree with the premise that data migration would ever be the prudent course of action in the event of a disruption believing that doing so would be far more likely to result in further IT risk and potential data loss. Members believe that it would be preferable in such instances to allow agreed incident management processes to progress and work towards resumption of services.

Regarding data classification, most firms maintain such a system internally. However, to include a qualification of what data would need to be returned in the event of a disruption would likely result in a significant project to reform that system which could disrupt ongoing efforts to improve data quality management. Most firms maintain a categorisation approximating, for example, public, internal, sensitive, highly sensitive for their data classification. However, such categories would not easily translate into the need to migrate in the event of disruption. For instance, high-sensitive data such as the firms annual results, minutes from the board meetings or sensitive client deals, may not need to be returned with any urgency depending on the time of the outage or if they were available elsewhere accessible to the firm.

In section 7.10 the PRA lists a series of controls that firms should implement for data security. While these are valid controls, they are not all appropriate at all times for all data. We suggest the PRA amend their text to say they "may include". Further, we note that the requirements for data security in 7.10 do not allow firms to take a risk-based approach by requiring that all data be subject to the listed controls when these are likely not all necessary, for instance in the event of publicly available data.

Members are of the view that dealing with the PRA in an open and constructive way should not extend to mandating the provision of encryption keys. We recommend 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.

Members also request an acknowledgement that it may not always be feasible for firms and regulators to have access to encryption keys. For example, if a cloud provider were to provide a key that has the potential to unencrypt the data of multiple unrelated clients using the same service. Moreover, members would expect strong challenge from the cloud provider in such a scenario, noting that cloud providers that operate on a 'one to many' basis are not often able to accommodate customer specific security requirements.

11. Access, audit and information rights

Alignment on this topic with the EBA GLs would be welcomed where feasible. However, on the subject of 'unrestricted audit rights' members would prefer language which mirrors the FCA's Cloud Guidance (FG16/5) which allows for a firm to provide "reasonable prior written notice of this visit, except when there is an emergency or crisis situation", as it is not always feasible for a supplier to grant full access and unrestricted rights of inspection and auditing. For example, some suppliers will impose fees or restrict the number of days per annum which are technically a restriction on the right to audit.

Additionally, some supplier information is sensitive and a firm's ability to obtain 'unrestricted access' may not be practical. For example, a supplier may only share a BCP if redacted in certain key areas or share examples of closed vulnerabilities rather than open vulnerabilities. Members would be grateful for the S/S to acknowledge that it may not always be possible, or indeed desirable, for suppliers to grant 'unrestricted' audit access.

Members would be interested in the PRA's view of when it is not possible for suppliers to obtain the same audit rights over fourth parties as the supplier is able to offer itself and for clarity on alternative ways to achieve compliance, as it is unclear if 'pooled audits' are an addition or alternative to the other direct audit rights. Additionally, they are keen to understand the PRA's views on how they would aggregate various decision outcomes from a single pooled audit.

Members welcome the workstreams being driven by the Cross Markets Operational Resilience Group (CMORG), which UK Finance co-chairs with the PRA. One of which is currently working on an industry solution to identify an assurance model that could fit the description of a pooled audit, although it is envisaged that it would act as an additional level of assurance rather than as an alternative. Planning for a pilot of this workstream is currently underway and CMORG will be briefed on it at subsequent meetings. In addition, through CMORG, UK Finance is actively encouraging firms to share best practice and common themes on supplier assurance.

12. Sub-outsourcing

An underlying assumption of members is that the due diligence of sub-contracting or sub-outsourcing of non-material outsourcing arrangements or other broader third party arrangements is not an expectation of the PRA, and that the requirement is only to understand sub-contracting or sub-outsourcing by the third party, rather than broader critical fourth parties that are not subcontracted or sub-outsourced.

Members would like clarification on whether the due diligence of fourth parties is the responsibility of the firm, or whether reliance can be placed upon the due diligence of the contracted third party. Additionally, members request acknowledgement by the PRA that mandating oversight of fourth parties will likely result in this requirement becoming overly burdensome when combined with normal due diligence processes undertaken by the contracted third party and have a significant impact on the costs and associated timelines of compliance.

Members are supportive of targeting this at 'material outsourcing' arrangements, as this 'scopes' the work, is risk-based, and pragmatic in terms of scale. But further confirmation that this is consistent with the principles of the operational resilience CP (and also noting the issue of timing with that paper), whereby understanding the impacts on important business services is not limited to just 'critical outsourcing' arrangements or sub-outsourcing / sub-contracting, would be welcome.

Members would also welcome acknowledgement that it can be challenging for firms to obtain consent for each sub-outsourcer in a supply chain, or to exercise termination rights where a service provider sub-outsources without notifying the firm beforehand. In addition, responses from sub-outsourcers can either be lacking or delayed, and sometimes it is not feasible for them to comply with all the contractual obligations in the primary contract. Members would welcome clarification that it would be sufficient for firms to terminate if there are reasonable grounds for concerns and request examples of what the "specific circumstances" (as per the S/S) could be.

Clarification is requested on how far into a service provider's supply chain monitoring is expected, including remediation efforts and acknowledgement that suppliers should only be required to use 'reasonable efforts' to do so. Examples of the forms of monitoring and expectations that would be deemed acceptable would be welcomed.

Members would like clarity on how far the PRA wants firms to go in terms of monitoring fourth party to nth party versus relying on due diligence by the third party. Given the challenge our members face in implementing a robust and effective third party risk management framework, they do not believe it is realistic to extend beyond fourth parties.

From an intra-entity perspective, it is queried 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.

Members are of the view that this would be an overly burdensome obligation considering the head office is responsible for such sub-outsourcing, and it is requested that the concept of 'proportionality' addresses this issue to lessen the compliance burden on members in this area. For example, 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. It is further requested 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.

13. Business continuity and exit plans

Members agree that the PRA should ensure that the requirement to develop an exit plan in the pre-outsourcing phase should be proportionate and realistic, with particular regard to the information available to firms in that phase. For example, the development of a comprehensive and granular exit plan pre-outsourcing may not be practical that early in the outsourcing lifecycle, given there will be a number of unknown factors at this stage. As a result, exit planning should not be linked just to pre-outsourcing. Existing outsourcing arrangements, by their nature, may well not enable a firm to switch over to another supplier in a cost-effective way and there will be accepted, managed risk within that arrangement.

It is more likely that a robust exit plan can be established in the transition period or within a period of time post-contract, which would make them more meaningful and impactful as firms will have a full understanding of the processes involved and therefore will be aligned to the actual service being provided.

Members are split on whether this time period should be at the discretion of firms or an indicative time period post-contract should be specified in the final S/S. Others ask that the PRA utilise the original wording from the EBA GLs on BCPs and exit plans.

It may be helpful for the PRA to clarify the 'outcome' it is seeking from the BCP and exit plan artefacts in each of the pre and post contract versions as what is possible is likely to be different at each point. Consequently, it should be acknowledged that exit planning, in particular, is an iterative process as arrangements are implemented and embedded.

Members would like to highlight the practical challenges, in some instances, of developing a fully scoped, costed, and tested exit plan to address risk of immediate failure (for example, liquidation) across all contracts. Therefore, a level of proportionality would be welcomed. Furthermore, it was highlighted that proportionate exit plans will also be required for scenarios outside of stressed scenarios (for example, commercial issues such as pricing, performance etc.) and that exits will still need to be managed in a way that promotes resilience.

The testing of exit plans is also an area of concern to our members. They are supportive of the need for credibility around their contingency arrangements but there are significant

limitations around the extent to which many plans can be tested. Clarity of the outcome sought and some 'good practice' examples would be welcomed.

14. Conclusion

We hope you find UK Finance's response helpful and we would be happy to discuss any of the points raised in further detail.

15. Responsible Executive

Ian Burgess
Director, Cyber and Third Party Risk
ian.burgess@ukfinance.org.uk
020 3934 1100