UK Finance response to the Bank of England and Financial Conduct Authority Discussion Paper 3/22 “Critical third parties to the UK financial sector”

Date: 23 December 2022

Sent to: DP3_22@bankofengland.co.uk

UK Finance is the collective voice for the banking and finance industry.

Representing more than 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

UK Finance, on behalf of our members, welcomes the development and adoption of this discussion paper. Mitigating systemic risks that may arise from third parties supporting the financial sector is an important consideration for the industry and we believe that, if implemented correctly, it has the ability to ensure that our members continue to thrive in a competitive marketplace, while building upon the relationships they have with those firms designated as critical third parties.

Our membership supports a phased and balanced approach by the Supervisory Authorities (SAs). Too little regulation may not have the requisite or desired impact, and too much regulation, or its imposition conducted too quickly, is likely to increase the risk of market exit by CTPs and reduce the competitiveness of the sector. We believe that largely the SAs have got this balance right.

The willingness of the SAs to engage with industry and our membership has been highlighted numerous times as being particularly helpful when introducing this discussion paper to its intended audience. Appearing at member events and fielding questions has allowed members to better understand the background and objectives of this paper. This regime is also not one that has surprised members thanks to the ongoing work of the Bank of England’s Financial Policy Committee (FPC) which has previously noted the potential risks that third parties can cause to the sector.

One of our ongoing advocacy priorities is coordinated regulation which integrates into existing frameworks, reducing costs and enabling transformation within firms, while promoting confidence that supervisors understand the issues that firms raise with them. It is for that reason that we welcome the introduction of minimum resilience standards and the alignment of this regime with the existing operational resilience framework introduced through SS1/21. This should help to ensure that material services provided by CTPs to firms are not overly disrupted by the introduction of this new regime or the resilience tests and sector-wide assessments that the regime envisages.

The designation of third parties due to concentration, materiality, and potential impact is appropriate and offers future flexibility. However, there is the potential for unintended consequences to arise from the designation of a firm as being a CTP. For example, where a firm is disinclined in wanting to become a CTP due to a perceived increase in their compliance burden, thus exacerbating concentration risk issues.

For this reason, we would encourage the SAs to designate a smaller subset of CTPs at the outset instead of implementing an overly expansive regime to allow this new regime time to bed in and adjust if necessary. Furthermore, the scope of the type of third party and service provided should be suitably wide to cover the full supply chain that underpins the provision of the material service when

considering the designation of CTPs. In essence, 'CTP' should not be synonymous with Cloud Service Providers (CSPs).

Finally, there is a positive consensus on the coordination with international supervisory authorities on the provision of material services by CTPs to firms, noting that alignment, the harmonisation of registers and other forms of standardisation could potentially make cross-border transactions more efficient. Furthermore, the introduction of a set of global resilience standards for CTPs would be a positive step. However, the magnitude of achieving this goal is not underestimated by firms.

Response guidance

To structure our response in the most digestible format it has been split into three sections.

Section 1 – A consolidated response to the 21 questions posed in the Discussion Paper.

Section 2 – Highlights issues that are not directly aligned with any single question from this list, but UK Finance's membership would like to be addressed.

Section 3 – A range of questions that our membership would like to be addressed by the Supervisory Authorities as they progress this regulatory journey.

Section 1

Question 1 - Do you agree with the supervisory authorities' overview of the potential implications of firms' and FMIs' increasing reliance on third parties (in particular the potential systemic risks to the supervisory authorities' objectives)? Is there anything else that the supervisory authorities should consider in their analysis?

UK Finance membership is broadly supportive of the SAs overview of the implications of the increasing reliance on third parties. There is an established consensus among respondents to the DP, that regulatory standards are a necessity to ensure that potentially systemic risks posed by certain third-party providers to the financial services sector and the financial stability of the UK are addressed.

It is only with this broad insight that systemic areas of potential concern, such as 'concentration risk' issues, can be observed and addressed. Concentration risk issues may manifest in the widespread adoption of a single CTP within the financial sector. Whilst the choice of third parties, would remain an individual business decision for the firm or FMI in question, the SAs knowledge of these concentrations could allow for more proportionate reliance measures and standards to be considered. Members are clear that their independence on the specifics of resilience measures taken is paramount and should not be dictated by the SAs.

Furthermore, members understand that the intention of the SAs is that firms' intragroup service providers and financial institutions that are regulated and supervised by non-UK financial services authorities are excluded from being designated as CTPs, and would therefore ask for the SAs to explicitly set this out in the forthcoming consultation paper and subsequent rules. Additionally, there is broad consensus that a third party supporting a small number of IBS of a small number of firms or FMIs should not be deemed sufficient for designation as a CTP as it would unlikely represent a truly systemic issue in the case of failure.

Members welcome that the DP rightly recognises that the applicability of the SAs measures need not be dependent on the location of the CTP or its infrastructure and personnel. Many CTPs provide global services. This global set up can provide benefits (e.g. greater resilience, 24/7 support etc.) to members, including many who themselves have global operations. Localisation requirements (whether they relate to entities, infrastructure, personnel, services or data) necessarily encourage fragmentation, which can lead to silos and lagging functionality. That said, UK Finance members have been clear that they would not support the development of extraterritorial powers by the SAs.

Question 2 - Do you agree with the supervisory authorities' assessment of the limitations of the current regulatory framework?

Among our respondents there is unanimous agreement with the supervisory authority's assessment of the limitations of the current regulatory framework.

Some members have further highlighted that a strengthening of the regulatory framework may increase the robustness of the standards for the whole industry. However, further assurance is needed that supervisory authorities are not unduly looking towards firms and FMIs as de facto regulators. Supervisory authorities should explicitly provide in the final rules that CTPs will be fully responsible and accountable for complying with all of their regulatory obligations and that they will not be able to delegate any of their responsibilities to firms.

Although this issue is not supported by all members, an industry led set of 'model clauses' on issues such as sub-contracting, scenario testing, OCIR responsibilities etc. may assist our small to mid-tier

members who inherently command less bargaining power individually and thus help maintain a diverse, competitive, and ultimately resilient financial sector.

Question 3 - Do you agree that, when considering potential requirements for CTPs, it is appropriate for the supervisory authorities to focus on (a) minimum resilience standards, and (b) resilience testing, in respect of the material services that CTPs provide to firms and FMIs? Are there any alternative or additional areas that the supervisory authorities should consider?

There is strong agreement that it is appropriate for the SAs to focus on requirements related to (a) minimum resilience standards, and (b) [relevant] resilience testing.

Having already produced the Supplier Assurance Framework, UK Finance in collaboration with CMORG, may be in good position to lead on standardised assurance testing that would consider the requirements of a broad slice of the UK based financial sector.

Question 4 - Do you agree with the potential advantages in aligning the potential measures for CTPs to the existing operational resilience framework for firms and FMIs? Are there additional ways in which the potential approach to CTPs could be aligned to the existing operational resilience framework? Are there alternative approaches the supervisory authorities should consider?

The alignment of measures to the existing operational resilience framework is supported by members. It is felt that there is potential for efficiency to be leveraged through this alignment that would benefit both firms and their CTPs. This must encompass alignment in practice, including definitions, terminology and processes. In particular, there is concern around the potential misalignment in some of the core facets of the framework, for example what is considered to be systemic or what is defined as a material service. We are particularly concerned about misalignment between what is identified by a CTP to be a material service versus what firms and FMIs have identified as an IBS.

There is some concern over the potential creation of a de-facto two-tier system, with some CTPs able to meet the regulatory requirements of a new, more rigorous, set of measures and some that are not and thus not able to continue to provide services to the financial sector. This in turn could have the unintended consequence of reducing diversity of CTP available to service the needs of the sector and result in greater concentrations among the bigger players. A gradual implementation or smaller designation of CTPs initially could reduce this risk. We would also encourage supervisory authorities to establish a formal review process for this framework.

The minimum resilience standards expected of the designated CTPs should align with existing operational resilience requirements. It is felt by some members that such alignment could help ensure that material services provided by CTPs to firms are not overly disrupted by the introduction of the new regime or the resilience tests and sector-wide assessments that the regime envisages.

Question 5 - What are your views on the factors that the supervisory authorities should consider when assessing which third parties to recommend for designation as CTPs? Are there any aspects of the criteria discussed above that the supervisory authorities should clarify, develop or omit? Are there any additional factors that the supervisory authorities should take into account?

There is broad consensus that the scope of the type of third party and service provided should be suitably wide to cover "the full supply chain that underpins the provision of the material service" when considering the designation of CTPs. In essence, 'CTP' should not be synonymous with 'CSP' and if it is evident that the service that a third party provides is objectively 'critical' a designation of CTP should be made regardless of the type or substance of service.

Members would encourage the SAs to consider a clearer definition concerning 'critical' or 'systemic' within the Discussion Paper. Further clarification of a designation would reduce risks of unintended consequences.

Question 6 - What are your views on the supervisory authorities' potential approach for assessing concentration, materiality and potential impact in the provision of third party services to firms and FMIs? Are there alternative approaches for doing so that could be more effective or pragmatic?

In addition to concerns over placing further compliance burdens on potential CTPs, the potential approach outlined in the discussion paper for the designation of CTPs is assessed by some member firms to be overly broad and ultimately may risk inappropriately including many third parties.

There remains a risk that there may be significant burden placed on firms to provide all relevant information for the designation of CTPs. A potential approach to first seek visibility over all material third parties across the financial sector, then focus on firms' Important Business Services and then overlay further information requirements to reduce the number of third parties designated. In any event, SAs should explicitly provide in the final rules that CTPs are fully responsible and accountable for complying with all of their regulatory obligations and that they will not be able to delegate any of their responsibilities to FIs.

There is an undercurrent of concern noted in the tone of many of the responses received to DP3/22 which suggest a fear of 'disengagement' whether wholly or in part (through the limiting of certain services) of some CTPs if they are feel burdened by regulatory requirements. As well as the substance of the changes, the concerns are articulated in terms of timescale of implementation. i.e. don't change too much too soon. These concerns are also echoed by an array of members in their answers to questions 4 and 8.

Where a CSPs is designated as a CTP we are aware that it will provide an array of services to a firm that all could respectively be designated as a material service (e.g. a CSP could provide 30-40 services for an individual hosted application which supports an important business service). Members would welcome further clarity concerning how a CSP's services would be designated in this instance. Any resilience standards or testing would need to take into account how all services together would interrelate for resilience.

Question 7 - What are your views on how best to take into account potential linkages with other regimes outside financial services when considering the recommendation of third parties as CTPs to HMT? How could the supervisory authorities improve coordination with other competent authorities and public bodies outside the finance sector?

UK Finance supports and encourages in principle the intention of the authorities to ensure sufficient collaboration and coordination with authorities and public bodies outside the financial services industry. As outlined in the DP, early collaboration will help the authorities to better identify the most pertinent linkages with other regimes and coordinate with counterparts appropriately, in order to better understand the impact of designation on both the third party in question and the economy more broadly. These potential benefits should be weighed carefully as part of the focus by authorities to create an efficient, proportionate and effective designation process. We recommend the authorities work with industry and counterpart regulators to determine a suitable governance process for cross-industry engagement, which should recognise as its foundation the respective overarching objectives and obligations of the relevant authorities and public sector bodies.

Question 8 - What are your views on how best to avoid or mitigate potential unintended consequences, including potential distortion, such as deterring third parties from entering the market or providing services to firms and FMIs, as a result of a third party being designated as a CTP?

Echoing the sentiment raised in previous related questions, members are concerned of any unnecessary compliance requirements being placed on them (as firms or FMIs) or their designated CTPs. Those fears are tempered by the recognition that this oversight framework is indeed needed to better mitigate the risks posed by the increased adoption of third parties in the delivery of their important business services.

The potential unintended consequences highlighted by respondents stem from a concern that, if not navigated properly, the design and implementation of a regime to designate CTPs and understand / control the risk they pose will lead to some CTPs exiting this sector of the market. A related, but not as severe, potential outcome of the same pressures is the possible reluctance of smaller firms to innovate and provide technology to the UK based financial sector if they are likely to be lumbered with a burdensome designation of 'CTP' and are unable to meet the associated compliance requirements. If either manifest, the likely second-order effect of both is a narrowing of outsourcing options available for members and thus increase the potential for concentration risk for those providers who remain.

We assess that it is likely that designation as a CTP will encourage firms and FMIs to consider that provider as inherently safer. This is to some extent desirable in that if designed well, the oversight framework should either provide greater assurance as to the resilience of the 3rd party or meaningfully improve their resilience. Either way, the firm or FMI would be justified in believing that there is a benefit to contracting with a CTP.

However, this is unlikely to be the main factor a firm considers when determining which Third Parties (TPs) to work with. The nature and quality of the service provision will still be the main consideration. Other factors, such as geographic availability (are they active in all the regions the firm or FMI needs) will also take priority. Only when comparing like-with-like services offered by 2 different TPs, is the designation of one as a CTP likely to influence selection, assuming the firm or FMI is still able to remain within its risk appetite.

For larger providers, such as Cloud Service Providers (CSPs), we believe that market competition among them would make it unlikely that they withdraw from serving regulated firms all together. However, there is a risk that, depending on the implementation of the regime, they may choose to limit the selection of services available to Firms and FMIs. For example, when rolling out a new

product a CTP may choose to limit FIs' access in order to avoid the product being identified as an important business service, and consequently subject to enhanced resilience requirements, before adoption reaches a greater scale.

There is also a product availability risk to FIs if a CTP is designated based on services provided to a single FI. In this situation, the business case for serving that FI could be significantly impacted and the TP motivated to withdraw a specific service from the FI in order to avoid designation. For some of the most material FIs, for instance FMIs, TPs, especially smaller start-ups with limited regulatory expertise, may avoid serving that market segment all together in order to avoid complicating their business model at an early stage.

There is an undercurrent of concern noted in the tone of some of the responses received from UK Finance members to DP3/22 which suggest a fear of 'disengagement' of some CTPs if they feel burdened by regulatory requirements, like the concerns expressed in response to question 4. A negative outcome would be if large systemically important firms having less choice of 3rd parties as this could result in reduced rather than increased resilience.

Question 9 - Are the supervisory authorities' potential resilience standards for CTPs clear, comprehensive and proportionate? Are there any standards that the supervisory authorities could add, clarify, omit or review?

UK Finance members broadly agree that the SAs' potential resilience standards for CTPs are clear, comprehensive, and proportionate. Members would like clarity on the governance approach required of the CTPs, to enable alignment with the expectations for firm's accountability for resilience. From a firms' perspective, new information received from supervisory authorities on CTPs should serve to enhance and better inform decision making and risk management in place, rather than create new obligations or requirements to continue usage of a CTP. Rather, any material new enhancements stemming from supervisory authorities' feedback should be determined and implemented by the firms themselves when, for example, they are made aware by the supervisory authorities that it is in breach of its regulatory obligations under the new regime.

Supervisory authorities should explicitly state expectations for CTPs on communication and cooperation with firms, linked to material services provided and in scope of the CTP regime, in order to reduce potential frictions and interpretations in this area which may deprive the new CTP regime of tangible benefits. Additionally, supervisory authorities should continue to support a risk-based approach to third-party oversight by firms. The proposed CTP regime, if effectively implemented and coordinated across jurisdictions, could provide firms with useful information to supplement existing due diligence practices. Firms should remain able to leverage their oversight frameworks with any intelligence received, whether from regulators, their own due diligence, pooled audits, or third-party audit reports, to help inform firm-level decision making and potential impacts to the firm.

Separately, while the final CTP standards are still to be determined, it is likely that new and potentially significant engagement may be necessary between a CTP and FI clients to implement certain aspects of the regime. In order to remove any potential frictions from differing interpretations of what is required, we encourage the UK regulators to explicitly state expectations for CTPs on communication and cooperation with FIs, for example, with regards to the development of FS playbook, among others.

Members would encourage that SAs agree on standardised protocol and data interchange formats as well as standardised metrics and measurement, to accurately assess risk and compare resiliency and availability between CTPs. Automation and centralised reporting should be implemented where possible, like that available for Open Banking.

Members would recommend that the requirements for CTPs to 'map' services should be made more prescriptive and require CTPs to include relevant dependencies and vulnerabilities across all material services. Mapping across all services will provide the most material benefit to regulated firms and the SAs, especially in relations to CSPs where a multitude of services are provided. An important consideration for mapping is how the material services interplay with other services offered to firms.

It is likely the case that most CTPs, for instance CSPs, will provide their services to not only a range of FIs, but also firms in many other sectors. The market's current understanding is that they do not have the ability to determine which firms are using which of their services at any one time. Therefore, they may not be able to develop a more tailored playbook for prioritizing recovery of certain services based on the customers using that service. However, one element of the CTP regime could be a pilot programme that assesses the feasibility of CTPs developing a tagging methodology that would give them this ability. Here, however, caution should be exercised. The only true way to isolate a specific sector's services would be to ringfence them from an operational perspective. Not only could this have negative impacts on FIs access to innovative services, but it could also result in even greater concentration within the CSPs operations creating a major critical point of failure for financial services. This would likely increase, rather than reduce, risk.

As with dependency mapping, input from FIs, whether bi-laterally or through industry groups, will be necessary to maximise the value of any CTP FS Playbook. This level of input will only be practical if the number of CTPs that result from a risk based designation process is very small.

UK regulators should also consider introducing robust governance requirements for CTPs similar to those imposed on FIs under Chapter 7 of the PRA Supervisory Statement 1/21. Effective governance arrangements, will help CTPs with managing their own operational risks and compliance with regulatory obligations, but it will also enable regulators to oversee and monitor CTPs' compliance in a more efficient manner.

Question 10 - What relationship, if any, should recognised relevant certification and standards have with the supervisory authorities' possible minimum resilience standards for CTPs?

Elements of UK Finance membership have expressed a view that taking account of recognised certification and standards could help to demonstrate resilience assurance, provide evidence, and reduce burden. There is, however, some divergence of opinion on what proportion of validation should rest on any individual CTP's offering of certifications or standard adherence; with some members questioning what value a new regime would have if it solely took account of existing certifications.

As such, external certification and standards should be considered by the SAs with due care and caution, to ensure that they do not become arbitrary measures of resilience or security posture which may not always be appropriate depending on the nature of the service provided, their limitations and overlaps. It is highly likely that the larger or more sophisticated firm's own frameworks are likely to be far more comprehensive than most external standards / certifications / accreditations.

As well as aligning to international standards, this approach could reduce the divergence between jurisdictions and reduce the cost of compliance for CTPs operating internationally. If this approach is taken, members would encourage SAs to make clear what certifications and standards are under consideration during this process.

Question 11 - What are your views on the potential costs and benefits of complying with the minimum resilience standards discussed in this DP?

Whilst members recognise the benefits of such standards enabling greater levels of assurance, members have expressed concerns that if compliance costs are considered to be excessively large, third parties could actively avoid becoming designated which would negatively impact the financial services industry and wider economy.

Implementing minimum resilience standards would result in increased costs for firms and FMIs which could ultimately filter down to the users of the services and potentially consumers. By allowing for the sharing of information, the regulators could materially decrease the regulatory burden for both CTPs and firms and FMIs. A suggested phased approach to compliance could ensure that the impact of implementing such requirements can be spread over a reasonable period, minimising impact to service costs.

Question 12 - What are your views on the potential resilience testing tools for CTPs discussed in this chapter? Are there any additional or alternative tools that the supervisory authorities could consider applying to CTPs?

There is a consensus amongst members for CTPs to perform testing using the same 'severe but plausible' ethos that firms are already using. This provides the assurance that is required and adds additional information to help firms design their resilience processes. In terms of "additional or alternative" tools, members have also suggested that information regarding data breaches, service failures or complaints by firms or FMIs against a CTP could be included.

Proposals regarding jointly testing CTPs and the SAs acting as coordinators are welcomed by members as it would reduce duplication and improve practical understanding. Automation of testing is also encouraged. Reporting of such testing and other materials could be disseminated by each provider via API, monitored centrally and reported where required. The specifics and limitations of this approach however would require further investigation.

The proposed testing tools should include a requirement for collective exercises, co-ordinated centrally by each CTP and joined on a voluntary or "opt in" basis by relevant firms and FMIs. This would form a pragmatic middle ground between individual functional / component testing and sector exercises (where firms, FMIs and CTPs are equal players), with the established benefits of a "one to many" approach

There are also examples of industry-led business continuity exercises that go beyond table-top scenarios. Examples here include SIFMA Classic[1], Reg-SCI[2] and FIA[3], all of which are designed to exercise market participants ability to failover from their primary to secondary sites, or other elements of their business continuity playbooks, such as communications. Two elements distinguish these exercises and make them useful models for a CTP scenario. First, the exercises test actual ability to maintain market services from either a disaster recovery site or in a situation in which the firms BCM playbook is activated. Second, the tests are not done in isolation, but with both FMIs and FIs present resulting in a high level of understanding and information exchange regarding resilience capabilities. While these exercises are tailored to market participants and therefore could not be directly translated into a CTP scenario, they do model the level of practical exercising and open collaboration to which any CTP exercising regime should aspire.

[1] https://www.sifma.org/wp-content/uploads/2022/07/2022_Industry_Test_Overview_Start.pdf
[2] https://www.sifma.org/wp-content/uploads/2020/04/SIFMAs-Reg-PlayBook-v.10192021.pdf
[3] https://www.fia.org/fia-disaster-recovery-exercise

Question 13 - How could the supervisory authorities work with CTPs, firms and FMIs and other stakeholders to make resilience testing of CTPs efficient, proportionate and resource-effective?

As all CTPs would, by definition, have been designated as "critical", UK Finance members have at this point not found agreement on what kind of testing regime should apply. (i) Some members believe that a single testing regime should apply, (ii) others believe that the testing regime should be proportionate and reflect the impact of the CTP on the financial system

Members have also suggested that by standardising the resilience tests, based upon industry best practices, this could enable third party firms to bid in a marketplace to carry out those tests for the CTPs, sharing resources and minimising customisation required for each CTP.

The SAs should consider undertaking a pilot exercise to test how the oversight framework could work in practice and finalise rules based on lessons learned and feedback from pilot participants.

The creation of groups looking at CTPs or relevant expert forums that promote and discuss the requirements of resilience testing would be incredibly useful to some UK Finance members

Question 14 - In terms of the different potential forms of cyber-resilience testing discussed in this chapter, are there any that could be particularly effective for CTPs? Conversely, are there any that could be particularly difficult to implement in practice or give rise to unintended consequences?

There is a strong, and well-reasoned perspective from elements of UK Finance membership that it is unlikely that CBEST will materially improve the resilience of the largest technology providers, such as the major CSPs. Additionally, this viewpoint sees risk (although minor) in any regime which may result in those CTPs prioritising low or minimal risk findings over strategic priorities simply because those findings carry regulatory weight.

It is noted that the largest CSPs already offer the ability for customers to conduct Threat-Led Penetration Testing (TLPT) on their deployments within the CSPs environment. The value in such testing would therefore come from targeting applications which firms and FMIs can't already test. However, it is assessed by some UK Finance members that it is unlikely for the provider to be able to test their services in such a way that is specific to a single FI or the FS sector. Any risk generated by a CBEST test will therefore be not to a single FI or the sector, but to all users of that service.

There is however, another view put forward by UK Finance Members who state that CBEST could serve as a good framework to test cyber resilience capabilities, as it has the capability to customise and incorporate various scenarios within the test strategy, which can be further tailored depending on the services provided by the CTP.

What might prove challenging or would have to be factored into the test approach, is the provision of secure sharing of the results (e.g., thematic reviews, analysis etc.) of the exercise with the industry participants. There should also be consideration towards keeping the participants appraised of key remediation plans, in which they could have a direct interest due to the nature and criticality of the services received from the CTP. We note that for cyber penetration tests such as CBEST, the results, including analysis and remediation plans are likely to be of the upmost sensitivity and therefore it is unlikely for the CTP to be able to safely share all but the highest level thematics outside of their organisation.

In addition, members have highlighted that additional cyber-resiliency testing may be resource intensive and expensive (such as simulating a DDoS attack). The availability of authorised third

parties to carry out such testing (and the locations from which they may work) may be significantly limited.

Finally, conducting these tests are resource intensive, including for the regulator. If the oversight regime is to include a significant number of CTPs then a requirement to conduct CBEST tests is likely to present a significant resourcing challenge for the UK authorities. The lighter touch FSTAR may present an option for scaling to a larger number of CTPs, but the decision to do so would largely be driven by resource constraints rather than a risk-based approach. The overall resilience of the sector would arguably benefit more from a more detailed and intrusive examination of the defences of a smaller number of the most critical CTPs than from a more cursory test of a wider number of CTPs.

Question 15 - What do you think could be the most effective way for the supervisory authorities to share the findings and recommended actions of any resilience testing performed by or on CTPs with, at least, those firms and FMIs that rely on them for material services? How could the supervisory authorities balance the need to share this information with relevant firms and FMIs with potential confidentiality or market sensitivity considerations? Could a rating system along the lines of the URSIT system used by the FFIEC in the US promote clarity and consistency in supervisory authorities' assessments?

UK Finance membership broadly support the high-level outcome that resilience information must be shared with the user community for the CTP requirements to be meaningful and provide in a more coherent manner the assurance that the firms, FMIs and SAs are looking for. There will need to be a clear requirement on CTPs for information sharing, potentially via a central body to ensure it remains objective and reaches an appropriate audience.

Some members have suggested that findings should be shared bilaterally as part of the contractual arrangement and oversight requirements. Members would like clarification if the SAs intend to share any findings in full or only the material issues/vulnerabilities, as well as how it intends to share the information with firms and FMIs. Furthermore, SAs should be mindful of any unintended consequences or negative impacts the framework may have on third party competition and innovation.

Members recommended that the CTP resilience testing consider a SIMEX model for the sharing of testing across regulated firms. SIMEX provides sector-wide feedback on the resilience of all firms. This could be reflected across designated regimes and offer an ability for the sharing of high-level testing information or shared themes across CTPs.

Question 16 - Could a set of global, minimum resilience standards for CTPs be helpful? If so, what areas should these standards cover?

Whilst there is a broad consensus amongst members for a set of global resilience standards, members are cognisant of the challenges associated with creating a global set of regulatory standards as well as the cost of compliance implications to firms. CTPs may provide material services to firms and FMIs in multiple jurisdictions and the potential systemic risks posed by their failure or severe disruption would not be confined to the UK. Furthermore, while other jurisdictions may introduce regulatory regimes which target similar outcomes, for example the EU's Digital Operational Resilience Act (DORA), there will be variations in the substance and scope from the UK's proposed approach which may create complications for both CTPs and for those firms and FMIs that operate cross-border. Members would also like to see a stronger encouragement of further work to support equivalence and coordination.

Members would welcome clarification from the SAs as to how they intend to create a global minimum resilience standard that does not create different sets of regulatory standards. Furthermore, there is no single regulator designated as final arbiter either in respect of the entire CTP population or in respect of individual CTPs. The SAs will be required to consult one another before issuing rules, gather information or taking enforcement action. Whilst the UK SAs have a track record of cooperation, particularly on enforcement activities, the robustness of these arrangements, in the face of a live disruption to a CTP, is untested.

Question 17 - What additional steps could financial supervisory authorities around the world take to enable resilience testing of CTPs to be coordinated effectively on a cross-border basis?

Close integration with communities such as the ECUC (European Cloud User Coalition) may help to strengthen co-operation and testing capabilities. It will likely be necessary to pre-identify test data, accounts and other information that can be safely used across borders without exposing actual customer data, so that jurisdictions with high data privacy requirements will be able to participate. Furthermore, the introduction and implementation of common lexicons and taxonomy would enable effective cross border resilience testing.

Cooperation should occur in situations where infrastructure is based in geographies outside of the immediate SAs' control, with consideration given to cross border prioritisation.

Question 18 - What forms of testing could be most appropriate (i.e. sector-wide exercises, TPLT or other forms)? Are there any practical challenges in these cross-border exercises which the supervisory authorities should anticipate and manage?

There are several views across members on forms of testing including thematic testing, sector-wide and cross-border exercises, as well as desktop or pooled audits.

While some members advocate for sector-wide exercises being reserved for the CTPs that would cause the most widespread impact across the financial sector, there is concerns that this approach may result in a de-factor two-tier CTP designation i.e. those mandated to undergo sector-wide exercises and those that are not. The benchmark for CTP designation should be significantly high to make this approach null and void as all CTPs should have widespread impact across the financial sector.

Cross-border exercises are likely to be costly and mechanisms of cost-sharing need to be considered and may only be possible with regulatory authorities with similar objectives. Targeted testing may need to be undertaken across firm types rather than just cross border, e.g., retail firm, wholesale.

There is a view that thematic testing should be based on rising risks [as opposed to established high risks] and that testing using this methodology could better prepare firms to respond to emerging risks and build appropriate safeguards. Pooled audits could be an effective way for firms and SAs to not only have a strong set of data to analyse the effectiveness of the CTPs providing material services but will also provide information on what enhancement can be made to close any identified gaps.

Question 19 - Are there any other ways not covered in this DP to improve international regulatory and supervisory coordination in relation to the risks posed by CTPs?

There is positive consensus among members on the coordination with international supervisory authorities on the provision of material services by CTPs to firms, noting that alignment and standardisation would potentially make cross-border transactions more efficient.

Whilst the DP does not reference a desire by the SAs to impose direct financial penalties on CTPs for non-compliance, it might be the case that other non-financial or non-UK financial SAs are willing to impose financial penalties for non-compliance, therefore SAs (as well as firms and FMIs) would benefit from being made aware of such penalties to manage any potential risks arising from the CTPs. In addition, standardisation of terminology would be helpful and operational resilience should not be only considered for technology and digital services. The impact of an engaged CTP failing to meet the standards during the life of an arrangement with a firm or FMI should to be considered. Mass exit from that CTP in response to an inadequate testing cycle will need to be managed carefully.

There is a need for further standardisation on the information that SAs request from firms via the outsourcing registers across different jurisdictions, so that firms are not required to maintain different outsourcing registers with different data points and formats. Such standardisation will improve the quality and reliability of the information provided by firms on their engagements with CTPs, which in turn will help SAs with their assessments of the potential impact of the failure or disruption of a third party's services on the SAs objectives.

On this basis and as part of the regulator's efforts to improve cross border regulatory and supervisory coordination, regulators should work together to (i) address the issues the firms have with the current data collection processes; and (ii) to ensure the least possible divergence in the reporting requirements of the various outsourcing registers with the aim of creating a global harmonised reporting model. A harmonised approach will improve the quality and reliability of the information provided by firms on their engagement with CTPs, which will in turn help regulators with their monitoring of the CTPs' systemic impact on the FS sector.

We also understand that there have been discussions regarding the creation by the SAs of Standard Contractual Clauses (SCCs). Model clauses, not mandator causes should be narrowly tailored and aim to address specific pain points/areas of concern. For example, firms frequently receive pushback from service providers when negotiating key contractual provisions relating to the firms' access, /audit and information rights, their entitlement to participate in the testing of a service provider's BCDR plan, termination rights and firms carrying out penetration testing.

Question 20 - What are your views on the possibility of the supervisory authorities taking into account resilience tests, sector-wide exercises and other oversight activities undertaken by or on behalf of non-UK financial supervisory authorities on CTPs?

On the basis that a standard format and accepted protocols are used, UK Finance members are broadly supportive of the SAs considering resilience tests, sector-wide exercises and other oversight activities undertaken by, or on behalf of, non-UK financial SAs on CTPs. It is accepted that this would aid compatibility and comparability to UK-based testing.

Industry-wide resilience exercises are an area where there is the potential to make progress on a number of key issues related to the possible systemic impacts of CTPs. However, there are a number of factors that would go into making such testing successful:

1. Exercises are resource intensive to organise and run. They also generate actions that demand potentially long-running resource requirements to address. Therefore, they are most suitable to the highest-risk challenges facing the industry rather than as a method of assurance.

2. The success of such exercises, including both the exercise itself and the follow-up actions to address identified weaknesses, depends on the willing engagement of the CTP. If viewed as a compliance or tick-box exercise by the CTP then the chances of meaningful progress are reduced and timelines are likely to extend.

3. Designing realistic scenarios that are relatively tailored to the CTP are essential to identifying real weaknesses or areas of further exploration. Some industry exercises have tried to operate based on scenarios that the participants did not consider realistic, or which were simply too large to allow for the identification of specific weaknesses. For example, past exercises designed around the scenario of the complete failure of a major CSP have not been successful at generating actionable results. Such a failure would have so many impacts, including far beyond the financial sector, that it is difficult for the industry as a whole, to engage with the impacts within the confines of an exercise. This is not to say that such a failure, however unlikely, is not possible. Instead, it is a comment on the way scenarios need to be designed to allow for the industry to engage in a more targeted set of impacts. An alternative to the total failure of a CSP could be to assess the impacts of the failure of a single major cloud region, or the failure of a specific service provided by a CSP such as their DNS. This approach necessarily means that it will require a long running exercise programme to begin to address the cumulative risk presented by the CTP. But this is nevertheless preferable to the big-bang approach which has been shown to yield inconclusive or unactionable outcomes.

These factors all suggest that any such industry-wide exercise programme would struggle to accommodate a large number of CTPs.

It may transpire that an incident which significantly affected another sector has an impact on the financial service industry and therefore it would be prudent for SAs to be aware of any weaknesses at the CTP and make aware the other sector regulators. A body of testing evidence covering a wide range of scenarios, would be needed to appropriately assess the resilience status of a CTP for this to effectively provide assurance to the financial service sector.

Question 21 - Are there any other areas besides those discussed in this DP where cross-sectoral cooperation could be developed to support the possible measures for CTPs discussed in this DP?

As with the answer to question 7, UK Finance membership have expressed a diverse set of opinions on this matter, with some considering wide collaboration as the best way forward and that this cooperation could be a benefit for both CTPs and firms as it may create efficiencies in relation to sharing of information. Other firms have expressed concerns over the potential delays if attempts are made to harmonise with other sectors as a part of this process. Any efficiencies in relation to information sharing can only be realised if there is a commonly agreed pan-sectoral approach to supervising resilience. In addition, wider coordination with the security services from a horizon scanning and threat assessment perspective would also be helpful, albeit if kept confidential.

Section 2 – Issues not directly covered within question format

Minimum resilience standards: There should be a consistent approach across CTPs, based on materiality assessments for specific services; a common service taxonomy provided by the SAs would be the best approach to achieve this and minimum resilience standards should be aligned with requirements on firms.

Proportionality: The PRA should extend or clarify its principle of proportionality (under SS2/21) to allow firms to factor the existence and output of new CTP resilience testing when framing the level and scope of internal third party resilience tests against the same population of regulatory designated CTPs.

Utilisation of Automation: Where possible, UK Finance membership would welcome the use of automation with the resilience testing process to reduce the burden on all parties.

Advertising and marketing: The Discussion Paper states that there is a risk that CTP designation may be used ultimately as a form of (at least passive) marketing. Taking the US-based FedRAMP as an example, it was never intended to be a badge of competence but it has nonetheless become one. While we acknowledge that a similar unintended outcome may occur in the UK, the SAs should from the outset strive to avoid this scenario, which otherwise poses potential risks to competition, innovation and concentration.

Avoidance of designation and negative impact: Where a CTP avoids the requirements by ceasing to have a UK incorporated entity the SAs need to consider the likelihood and impact of this scenario. As a continuation of this theme, members have commented that it is highly unlikely that CTPs would ever allow themselves into the position where they are forced from the market due to the SAs sanctions. It is highly likely that CTPs will remove themselves from the market before any adverse regulatory response forces their hand.

Practical considerations on testing withing the cloud environment: Consideration should be made to the risks and nuances of testing in a multi-tenant environment that will be particularly relevant for some CTPs e.g., cloud providers. Getting the framework right for this environment will ensure that unintended negative consequences leading to business continuity and resilience failures don't materialise. Lifting and shifting traditional testing methods and frameworks (like CBEST) will not necessarily be appropriate.

Removal of a CTP designation or gradual designation process: A CTP could reduce its level of material services across regulated firms over time and therefore no longer be considered a CTP. The SAs should provide an instance of how a firm would be removed from the regime. In addition, the CTP should have a period by which it has time to comply with the regime's new standards.

Section 3 – Questions for the SAs for clarity from members

- What are the SAs intentions in the future in terms of requesting firms CTP listings e.g., frequency of submission and format?

- Would the SAs intend to share the outputs of CTP self-assessments with firms (referenced as a potential solution in section 3.7) or will it be limited to the results of resilience testing?

- Members propose that the SAs consider a gradual implementation or a reduced number of CTPs being initially designated. There is a material risk that the regime could result in significant number of CTPs being designated and this being highly difficult to oversee for the SAs, with a varying degree of systemic impact. There are a number of CTPs, with a clear systemic impact, that are highly likely to be designated and will entail a high degree of work to oversee. Members suggest designating these providers first before committing to a far wider regime. Members would welcome clarity from the SAs on the issues raised in this paragraph.

- Will there be a regulatory mechanism that firms can invoke to ensure that CTPs provide accurate and up to date information?

- There is a need for a clear definition in the gradient of "severity and plausibility" required to ensure all firms and suppliers are consistently testing and proving resilience, or not. Members would welcome clarity from the SAs on this point.

- There is some ambiguity in how the proposed framework will work in practice and further clarification from the SAs would be welcomed on the following:

- A number of third parties that are expected to be designated as 'CTPs' are currently not regulated by the SAs and as such they may not be familiar with the SAs objectives. There is therefore some uncertainty as to how CTPs will be able to identify fully and accurately the services that could have a systemic impact on the SAs objectives ('material services'). This raises the question on whether firms will be expected to be validating CTPs' identification of material services, particularly since there is no full alignment between the Important Business Services and material services.

- We understand that the entity to be designated as a CTP will be the entity providing the service(s) to the UK firm. The entity providing the service may be a third-country CTP and as such it is unclear how the SAs will ensure an adequate oversight of third country CTPs and how they will be exercising their powers over them;

  (i) how will the designated CTPs be notified to firms?
  (ii) will either the SAs or HMT publish and update the list of CTPs
  (iii) will an obligation be put on CTPs to notify firms when they enter a contract with them; and (iv) what will be the frequency of the review of determining whether a third party meets the CTP designation criteria;

- The consultation notes in paragraph 4.4 (page 23 of the DP) that "certain third party providers of non-ICT services, e.g. claims management services to insurers or cash distribution, could also be considered for designation as CTPs if they were deemed to meet the proposed statutory designation criteria." We would value further clarification from the FCA on specifically what services they were intending with respect to claims management services to insurers or cash distribution as it is currently unclear. We note the existing provisions in the Financial Services and Markets Bill with respect to wholesale cash distribution and would value clarification on what 'cash distribution' services the FCA's was intending beyond that.

If you have any questions relating to this response, please contact Adam Avards, Principle Cyber & Third Party Risk at adam.avards@ukfinance.org.uk

Adam Avards
Principle, Cyber & Third Party Risk