DP3/22

techUK’s response to the PRA/FCA Discussion Paper DP3/22 on Operational Resilience and Critical Third Parties

December 2022

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet.

It is the UK’s leading technology membership organisation, with more than 900 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

For more information, contact Head of Financial Services, techUK, Andy Thornley

E: andy.thornley@techuk.org

**Key points**

* The PRA/FCA should consider recognition of, or ‘equivalence’ being granted to the obligations, such as under the Telecoms Security Act and associated requirements where appropriate;
* For many CTPs, it may be difficult to ringfence only their services that pertain to FSIs as they are ‘multi tenancy’. Therefore regulators and Government need to understand the scope proposed by this work extends far outside of just financial services;
* Regulators should consider allowing a ‘reading room’ for accessing documents and information rather than holding it themselves and share only the result of assessments of resilience (such as pass/fail/needs improvement) with FSIs.

**Questions**

**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?**

We agree with the broader overview of the potential systemic risk to the regulators’ objectives; however, there is an important distinction to make. The paper makes reference to ‘single points of failure’:

*2.9 Disruption to any material services that certain third parties provide to firms and FMIs could therefore lead to a single-point-of-failure that that may simultaneously impact:*

* *multiple firms and FMIs;*
* *these firms’ and FMIs’ counterparties, customers and/or direct participants (even if they do not directly rely on the relevant third parties’ services); and*
* *in extreme cases, the financial stability of the UK.*

Whilst there are single suppliers who are critical to firms and FSIs, they are by no means a single point of failure. For example, Cloud Service Providers (CSPs), have multiple resilience measures to ensure the any single point of failure is reduced to such an extent, it is minimal. The same is true for other providers in areas such as networks, data and telecoms. Consideration should also be given to multi cloud options which have been increasing in the industry and reduce concentration risks.

In addition, telecommunications providers play a critical role in the supply chains of many FS firms and FMIs and they work closely with these customers to support their resilience planning. Telecoms providers are already closely supervised by Ofcom, with guidance from the National Cybersecurity Centre (NCSC) under GCHQ. They are subject to multiple existing regulations and requirements which already regulate telecommunications providers as Critical National Infrastructure (“CNI”) and/or regulate our resiliency and security, e.g.

* The **Telecommunications Security Act (“TSA”) 2021,** which is closely supervised by Ofcom and NCSC/GCHQ;
* **Ofcom General Conditions of Entitlement**, which act as baseline licencing conditions for operating in the UK;
* **Network and Information Systems Regulation 2018** – as Operators of Essential Services and Relevant Digital Service Providers;
* **Investigatory Powers Act 2018**, which governs our engagement with intelligence agencies and law enforcement;
* **System and Organisation Controls (SOC) for Service Organisations** and **ISO standards** based.

The potential application of operational resiliency requirements from the BoE/PRA/FCA **duplicates existing requirements,** particularly under the Telecommunications Security Act, and **creates uncertainty in terms of supervision and enforcement,** the primary role for which should remain with Ofcom and NCSC/GCHQ. Alternatively, telecommunications firms could be excluded from designation for their non-FS regulated businesses.

Furthermore, clarity is needed on the strategic and operational benefit of the regime, including the following areas: 1) ownership of systemic concentration risk; 2) changes in the expectations for firms when conducting due diligence of CTPs; 3) contribution to resilience testing of CTPs; and 4) information from the resilience testing of CTPs. Specific guidance that a multi-vendor strategy is a part of a range of options including CTPs and non-CTPs and is not required would be beneficial.

That said, we do welcome the principles-based approach to this work and agree there is a role for oversight in this area where businesses have an FS-regulated business portion of their work regulated by an FCA licence or permission.

**Do you agree with the supervisory authorities’ assessment of the limitations of the current regulatory framework?**

We agree with the statement that responsibility cannot be outsourced and currently, there is limited scope in the current framework for the regulators to satisfy themselves of the resilience of CTPs across the board. However, caution must be applied when remedying this limitation given the fact most, if not all, of the CTPs potentially in-scope are not carrying out any regulated financial activity and are cross sectoral with a broad range of service offerings. This can present difficulties with regards to ring-fencing operations and approaches to specific sectors, something we discuss further in our response to this DP.

**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?**

We agree with the premise of the question that requirements should only relate to ‘material services that CTPs provide to firms and FSIs’. Ensuring materiality will be an important principle to hold at the centre of the rules which will be drawn up in this area.

However, there is not enough detail as of yet to determine what regulators will consider as material and, as discussed below, it is difficult to ringfence just those operations which relate to FS firms as many services, such as cloud, are multi-tenancy and it is typical for CSPs to provide a wide variety of service offerings where not all should be deemed “material”.

With regards to the requirements for material services, we agree that where they apply to a CTP, they should relate to (a) minimum resilience standards, and (b) resilience testing. However, caution should be exercised and the CSPs should be involved in the process of defining such standards to ensure they do not create more security risks in requiring the time and effort of the CSPs to be focused on reporting/updating/conducting testing exercises for the authorities rather than focusing on the effort needed to security the cloud services. There should also be consideration given to requirements around access to information so as not to increase risks to security by provision of sensitive information which could cause more harm to the CSP’s services and customers if such information were to be obtained by the wrong people.

**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?**

There are obvious benefits in both frameworks for CTPs being aligned to those of FSIs, given the role CTPs play in enabling key functions and services to operate. Indeed, aligning frameworks is likely to ensure more effective oversight and reduce the opportunity for aspects to fall between the gaps. Following a risk-based approach which is based on firms own risk assessments; alignment to industry and non-financial services standards to support consistent adoption; technology and provider agnostic; and a regime that is operationally feasible for both CTPs and firms that does not stifle innovation will ensure an effective regime.

However, great care must be taken to ensure that, especially where CTPs operate cross sector, due regard is given to existing regulation and/or oversight to avoid duplication or specific requirements which pertain to those aspects of service which relate only to financial services – something which would be very difficult in practice to achieve for many CTPs.

We give examples of regulatory duplication below:

|  |  |  |
| --- | --- | --- |
| **CTP** | **Communications Act as modified by TSA** | **NIS** |
| Identification | Pre-requisite to further stages | N/A |
| Mapping | Requirement to record type, location, software/hardware information of equipment, review processes | N/A |
| Risk Management | Must identify and reduce risks and prepare for occurrence of security compromises | Must take appropriate / proportionate measures to manage risks to security of the network |
| Testing | Must carry out test to identify the risk of compromise. Must simulate techniques used by real-world threat actors | N/A |
| Engagement with supervisory authorities | Must inform Ofcom as soon as reasonably practicable of security compromise, must provide information under S.135 processes | Must notify designated competent authority about any incident which has a significant impact on the continuity of essential services, including the number of users affected, duration etc. |
| Financial Sector continuity playbook | N/A | N/A |
| Post-incident communication | Duty to inform users of risks of a security compromise | N/A |
| Learning and evolving | N/A | N/A |

It is notable that where there was duplication between the security provisions of the Communications Act and NIS, Government took the decision to exempt communications providers from NIS to the extent that the Communications Act already provided regulatory oversight.

**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?**

Aside from the argument for equivalence, argued elsewhere in this paper, the broad criteria for CTP set out appears to achieve the policy objective. Whilst we recognise that this discussion paper is the beginning of the process, more detail will be needed for providers who may be in-scope to understand more. This should include clear criteria and parameters for assessments and recommendations by the regulators and a further well-structured consultation between the providers in scope and regulators as rules and criteria are being developed.

It would also be helpful to clarify whether the supervisory authorities intend to re-assess service providers periodically, for example annually, for the purposes of identifying CTPs in order to take into account changes that may affect whether a service provider meets the criteria for being designated as a CTP.

This consultation should also provide oversight plans, current recommendations, and remediation mechanisms before rules are finalised. The purpose of this would be to avoid any disproportionate or non-workable recommendations. techUK will gladly facilitate any meetings with providers who may be in-scope as many will be within our membership.

**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?**

The high-level approach outlined is a sensible one; however, members are keen to understand more detail of how this criteria will be determined, how the recommendation will be made and on what basis HMT will make the decision (i.e. do they consider any other criteria or simply take the recommendation made by the PRA). Without this detail and opportunity to help shape it, it is difficult to comment further.

techUK also welcomes the assessment that few in number will be in-scope of this work with the indication it will be only those providers who truly are critical to a FSIs.

**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?**

This is a crucial question and should be at the heart of Government and all regulator’s minds when forming policy which cuts across several sectors. Some members raise concerns that the new regime, however well intentioned, gives very broad powers to the regulatory authorities over third parties on a par with the powers the regulator currently exercises over the firms.

Digital and data services, by their very nature, run though almost every sector of the economy and there is a risk that regulators in different sectors take separate approaches which would amount to dual/poly regulation. Many of the providers who will be in scope of the CTP rules offer services to more than one sector and ring-fencing an approach or playbook to just one sector, in this case financial services, is not something which can be done. Conversely, care also needs to be exercised in the wording of the rules to ensure that the scope does not creep to a corporate level, especially where other services may be offered by a CTP. With this in mind, we recommend only regulating those services designated as being ‘critical’ with clear definitions and explanations to provide clarity and certainty. We also suggest the FCA/PRA seek to align the methodology with the Delegated Act under DORA which indeed will define the criteria and methodology for designation of CTPS.

Early sight of the mechanisms and detail of scope, testing etc will allow potential conflicts between the regulatory requirements of different parallel regimes (eg EU DORA, NISD2 and UK NIS) to be identified more quickly.

As above, it should be made clear that where superseding regimes (such as the TSA) already apply, the primary regulators for those regimes (such as Ofcom and GCHQ) should remain the primary supervisors, or that such firms should be excluded from designation.

Finally, information returns to regulators also need to be better shared in the regulatory community to ensure that the same or similar requests for information from providers in scope are not duplicated.

**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?**

In creating a regime for CTPs where certification is required, there is a risk of creating a high-bar to entry for firms offering similar services to those of CTPs. One way of promoting competition would be to consider the regulatory requirements placed upon FSIs and to consider how these might differ if they were to use a provider not designated as CTP.

**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?**

techUK members who might be in-scope do not feel that the specifics with regard to oversight are on their own burdensome or disproportionate; however, as discussed earlier in this response, the multi-tenancy nature of services such as cloud means that regulations reach outside of Financial Services. Members state this is because it is not possible to ring-fence just services that are provided to FSIs and therefore any requirements have the potential to affect a provider on a corporate level, as well as other customers who sit outside of financial services. Providers feel that this has the potential to be disproportionate and a clearer route to regulating such services, where they cut across multiple sectors, needs to be found through further consultation. However, other members highlight that resilience solutions such as escrow agreements exist which might easily accommodate multi-tenancy services.

Certain of the proposed resilience standards set out in Table C in the Discussion Paper suggest that CTPs will be in a position to determine whether disruptions or incidents affecting the services they provide will have systemic impacts on the supervisory authorities’ objectives. It is unlikely that any single CTP is likely to have the information or level of visibility required to determine the extent to which the disruption to a particular service would have a systemic impact. The minimum resilience standards should make it clear that it is the role of HMT, in cooperation with supervisory authorities and in consultation with potential CTPs and FSIs, to identify which services are material according to the specified criteria.

Finally, members have also expressed a view in terms of how these standards can remain ‘future proof’. Regulation and supervisory practices should evolve in line with digital practices and advances so that the supervisory framework continues to be effective and efficient as technology matures, while maintaining the highest level of security of both providers and financial institutions. As an example, supervisory authorities may consider harnessing new or evolving solutions that do not create security risks for both CTPs and their customers when gathering and handling evidence as part of their supervision, both within the financial services sector and beyond.

**What relationship, if any, should recognised relevant certification and standards have with the supervisory authorities’ possible minimum resilience standards for CTPs?**

As discussed in answers above, we suggest that equivalence, where the existing standard is both robust and appropriate, be considered instead of inclusion of this regime. This would ensure proportionality and would not necessarily exclude providers in participating in resilience exercises to test and learn from various scenarios.

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

Given the high levels of operational resilience and minimum service levels that service providers to FSIs are required to achieve under their contractual commitments, direct costs may be similar to those already faced by these firms.

However, indirect costs could be significant. For example, if telecoms firms were to be in-scope, they would need to re-contract with their client base, an exercise which we have been told by members would be estimated to be in the region of seven figures and significant time and resource to achieve. This exercise would not achieve any significant benefit for the huge cost and effort required to complete this. For this reason, we believe that serious consideration should be given to accepting ‘equivalence’ of existing requirements, such as the Telecoms Security Requirements (TSR).

Nevertheless, other members have noted that one potential solution could be to require regulated firms to deliver the changes necessary to supplier contracts when their contract term comes to an end or is up for renewal which may avoid costly re-contracting. Some members also argue that the operational resilience objectives of the Financial Services and Markets Bill go further than those outlined in the TSRs and other associated regulatory regimes such as NIS, and that therefore – while there may be scope for compliance with (e.g.) TSRs and NIS to demonstrate partial compliance with PRA/FCA’s regime – additional measures will likely need to be implemented to effectively manage the risk to the UK financial system.

**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?**

In relation to scenario testing, the DP states that it might be reasonable to expect CTPs’ scenario testing to be “at least as sophisticated as that performed by significant firms”. The supervisory authorities should take a proportionate approach when assessing the adequacy of a CTP’s scenario testing, taking into account that a CTP’s scenario testing might reasonably focus on the specific material outsourced functions it performs and consequently be less sophisticated than the scenario testing of an FSI that might cover broader business operations.

**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 suggested above, a proposed ‘equivalence’ would ensure greater regulatory cooperation in terms of oversight, but still allow those CTPs to participate in sector-wide exercises.

**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?**

We have chosen not to answer this question.

**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?**

This is a key concern of members. Information requested by the regulator could be commercially sensitive or feature sensitivities in terms of security or confidentiality. It is some members’ strong preference that information such as this is not held by the regulators, but providers can have the option to provide a ‘reading room’. This is where the required information is made available to be viewed, but not removed from the host’s servers. The purpose of this would be to ensure the added security and concern about commercially sensitive information being held on a competitor’s cloud services for example.

In terms of sharing this information, again there is concern as to what would be shared. Members have suggested that regulators could simply offer a pass/fail/needs improvement style rating to FSIs, rather than share with them reports which would reduce the risk of information accidentally being shared. Such a rating would not be a score or a league table, but instead would indicate the regulators’ satisfaction that the required standard has been reached. Creating a scoring system or similar would be a significant departure from how FSIs themselves are regulated which would raise significant concerns amongst CTPs.

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

As most, if not all, providers who might be in-scope operate as global entities, any resilience standards needs to align with existing requirements, especially where it is not possible to ring-fence the service solely to FSIs. Existing standards to consider include EU DORA, NISD2 and UK NIS.

**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?**

**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?**

**What forms of testing could be most appropriate (ie 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?**

We have chosen to answer these three questions together.

We were pleased to hear from the FCA that international coordination with the Financial Stability Board, Basel Committee on Banking, CPMI – IOSCO, G7 Cyber Experts Group, International Association of Insurance Supervisors and other national/regional initiatives such as DORA have already been identified. However, what members are lacking at the moment is any detail on how the regime fits with these regulators or initiatives. We understand that the discussion paper is one of he first steps in helping to shape policy, but members would like more detail on this and the opportunity to input as policy/rules progress.

**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 (subject to certain conditions)?**

As described above, we believe that an ‘equivalence’ should be considered for robust and appropriate oversight where it exists. It would be prudent to take in to account exercises and tests from other sectors; however, there is still value in exercises that involve all significant parties of the supply chain to ensure that resilience testing is both realistic and does not create a risk of a ‘blind spot’.

**Are there any other areas besides those discussed in this DP where cross-sectoral cooperation could be developed to support the possible**

There is still ambiguity around how bodies including the soon-to-be-formed Digital Markets Unit, Information Commissioner’s Office and Better Regulation Executive will have a role to play in this work, given there are significant areas of interest for each. More clarity in the design stage of these rules would ensure that oversight is both proportionate and not duplicated.