Date: December 20, 2022

To: The Recovery, Resolution and Resilience Team
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA
Email: DP3_22@bankofengland.co.uk

From: Andrew Moyad, CEO, Shared Assessments LLC
amoyad@sharedassessments.org
+1-505-466-6434

RE: UK Prudential Regulatory Authority Operational Resilience DP3/22 Discussion Paper
Shared Assessments Regulatory Response

The Shared Assessments Program appreciates the opportunity to submit comments to the Bank of England Prudential Regulation Authority.

Shared Assessments has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body which defines best practices, develops tools, and conducts pace setting research. Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy, and business resiliency control assessments. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org.

On behalf of the Program and its members, thank you for accepting the following response in regard to Operational Resilience DP3/22 Discussion Paper.

UK Prudential Regulatory Authority Operational Resilience DP3/22 Discussion Paper
Shared Assessments Regulatory Response

1. (part 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)?

RESPONSE: We agree with the supervisory authority's perspective that financial institutions' increased reliance on fiduciary management firms and other Critical Third Party (CTP) providers in complex sourcing chains—often characterized by increasingly significant third party concentrations—poses a potentially substantial risk to the UK's financial sector.

RATIONALE: The implications of the cascading concentration risk from increasing reliance on third and Nth parties has become a front burner issue that poses a threat requiring assessment and management of the potential systemic risks associated with that reliance. Accordingly, regulators in many jurisdictions have placed an increasing level of importance on the maintenance of easily accessible, regularly updated, robust third party registers. The issues covered by the Discussion Paper are complicated by the lack of harmonization across jurisdictions as authorities work to regulate these risks.

1. (part 2) Is there anything else that the supervisory authorities should consider in their analysis?

RESPONSE: Two additional areas could be considered in the supervisory analysis: (1) formalize the provision in the PRA's Supervisory Statement|SS2/21 Outsourcing and third party risk management March 2021, PS7-21 Section 5.13 to ensure within this new regulation that a portal is created and maintained that supports the PRA right to audit material service providers; and (2) clarity in the criteria for how CTPs are defined.

RATIONALE: With reference to right to audit, the PRA reinforced in its March 2021 guidance certain high level expectations around CTPs. While firms are working to adhere to this guidance, not all firms may be readily able to gain visibility into the cascading sourcing chain risks. The supervisory authority might achieve this insight based on the information collection and sharing model described in this Discussion Paper for materially significant entities, which could result in mapping CTPs by function and role within the supply chain.

The March 2021 guidance demonstrates that firms must contractually establish the right to audit material providers. This is clear in the requirements of Section 5.13, which states *"the PRA intends to publish a subsequent consultation setting out proposals for an online portal that banks and insurers would need to populate with information on their outsourcing and third party arrangements or a subset thereof, such as those deemed material."* Further, in section 7.3 of this document, *"the only substantive addition the CP* [Supervisory Statement|SS2/21 Outsourcing and third party risk management March 2021, PS7-21] *proposed was that in light of the PRA's operational resilience policy, the PRA would expect the written agreement to include provisions regarding the testing of business continuity and exit plans, which should take account of firms' impact tolerances for important business services. This expectation has been retained in the final policy because without the inclusion and co-operation of outsource providers, firms will be unable to test their ability to remain within their impact tolerance during a period of operational disruption."* Further, section 7.4 notes*: "The minimum contractual safeguards set out in the SS are essential to ensure that key provisions in other chapters of the SS, notably access to audit and information rights, data security, and business continuity and exit plans, are rendered contractually effective. Moreover, the imbalance in contractual power between a small firm and a dominant service provider should not be considered as justification for a firm to accept clauses and terms that do not meet legal or regulatory expectations. This principle is set out in financial regulation and other areas, such as data protection law."* Sections 9.2 and 9.3 provide for *"unrestricted audit rights." The PRA has made the effort to "in line with the original policy intention, the language around access, audit, and information rights has been reviewed and updated to ensure consistency with the EBA Outsourcing GL… The PRA expects that firms should retain their underlying right to conduct an onsite audit. For material outsourcing arrangements, the PRA expects firms to inform their supervisor if alternative means of assurance have been agreed."* We recommend that the PRA formalize these provisions to more fully support firm's setting contractual right to audit requirements with their critical third parties.

Regarding criteria for CTPs to be effective, we recommend the definition be expanded beyond the primary cloud and sector utility provider market examined in the Discussion Paper to include other service areas where CTP's are used (e.g., SaaS and other application hosting). Information also needs to be available to identify single source providers that escalate risk through a single point of failure that would be catastrophic to the system (such as SWIFT or Euroclear). Consideration should be taken into the impacts of mitigation methods being applied for this problem, which increasingly includes the mitigation trend using data sovereignty to attempt to manage issues where risk that an individual firm might be able to absorb cannot be accepted by the sector as a whole.

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

RESPONSE: Yes—in part—as a high level regulatory supervisory framework should bring standardized guidance for all organizations operating within the financial sector. The current framework does not ensure that risks of ambiguity and interpretation are minimized. If regulators establish a standard that the suppliers have to meet, our recommendation is that this standard extend to third and fourth parties (and Nth parties as appropriate), with deeper examination if critical parties are discovered further down in the supply chain that meet the Finance Authority definition of a CTP.

The lack of transparency into the supply chain is a severe limitation in the finance sector, where the onus for resilience lies entirely on the FMIs and firms without the practical ability to exercise audit rights against down chain providers. This regulation would provide supervisory authorities with a way to mitigate this situation by exercising the right to monitor critical services identified during the authority's mapping process.

RATIONALE: This new regulation is a natural extension of SS1/21 Operational resilience: Impact tolerances for important business services and would be expected to impact policy for the wider sector, which would naturally exert a ripple effect that—at its best—would provide value to firms, the sector as whole, and to the public. Through it, the PRA will be able to provide greater visibility into supply chain providers in ways that will allow outsourcers to gain information about services that are not currently readily available at the outsourcer level—which will further assist firms that have mapped the resources they need to remain within their tolerances based on the information they are currently able to obtain.

3. (part 1) 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?

RESPONSE: We agree that a minimum standard of resilience should be laid out and guidance/requirements published for CTPs to follow in respect to material services. Reporting should be made to the authorities against these standards on a basis determined to be sufficient for the service provided (e.g., continuous monitoring may be appropriate for supervisory authority given the nature of services that some CTPs provide). We recommend principle-based regulation, which would be expected to provide stakeholders with a stronger foundational starting point for rules, as well allowing the PRA to construct models of the third party ecosystem around what is considered "material" and what is not; as opposed to more prescriptive-based regulation. In the event that supervisory authorities intend to provide a sector-wide critical services map, it should be managed by the regulator in a way that provides visibility without disclosing IP/confidential components of products/services. This would be expected to influence supplier selection by outsourcers, which could have both positive and negative knock-on impacts.

RATIONALE: The Discussion Paper appears to recognize that a middle-ground approach would establish an initial set of rules with a defined structure that can be administered and tested with the expectation that adaptations will be needed and accepted through a feedback process as key data points for reporting are established and it is determined how the data set can best be utilized from a sector perspective. Defining the requirements by service type would also be of benefit.

3. (part 2) Are there any alternative or additional areas that the supervisory authorities should consider?

RESPONSE: We recommend that authorities consider how to include guidance covering testing and requirements to verify contracted (Service Level Agreement—SLA) recovery times can be met for severe, but plausible events. Recovery times must be appropriate to industry requirements (in effect, industry level impact tolerances) needed to maintain stability. The regulation could reiterate the

Supervisory Statement SS1/21 mandate that "*scenario testing should not pose risk of creating/resulting in material disruption.*" Minimum resilience standards could include mandated redundant services (as per Supervisory Statement SS1/21) that are frequently tested and can serve as an "auto-failure-response regime" during loss of key services.

RATIONALE: Common criteria should include components based on service type and best practice such as: the type of data being shared; the method of data transmission; the physical location of the data (including any movement to sub-outsourcers); type of systems being accessed and method of access; and availability requirements for the service. While critical infrastructure such as public utilities would fall outside the scope of this rule, the PRA could encourage enlightened organizations which might be interested in investigating alternative sources or methods in maintaining functions for power and communications when primary providers are disrupted.

4. (part 1) Do you agree with the potential advantages in aligning the potential measures for CTPs to the existing operational resilience framework for firms and FMIs?

RESPONSE: Yes, any new regulation should be expected to impact policy for the finance sector and to work in concert with SS1/21 Operational resilience: Impact tolerances for important business services.

RATIONALE: Alignment with prevailing practice facilitates and simplifies compliance for the supervised firms.

4. (part 2) Are there additional ways in which the potential approach to CTPs could be aligned to the existing operational resilience framework?

RESPONSE: Expanding the existing Red/Blue team testing to a sector-wide approach would be useful for supervisory approaches to testing.

RATIONALE: To date, regulator-initiated testing scenarios have been entirely based within the UK marketplace where involvement has been considered voluntary. This testing process could be extended as a mandatory process for financial sector firms in which the PRA works with a committee to see what types and scenarios would be effective for testing and when those would best be applied. In this construct, and with cross-sector for CTPs and cross-border agreements: (1) the regulator is able to choose the area/environment; (2) a consultation between the firms and the regulators establishes how/where testing takes place; and (3) results are shared through the provider to the larger industry (and the regulator normalizes the data).

4. (part 3) Are there alternative approaches the supervisory authorities should consider?

RESPONSE: We recommend that the supervisory authorities review the full range of testing processes that are currently being applied by firms in order to guide robust testing hygiene and reporting processes and reporting (as appropriate). For example, SWIFT has historically managed a mandatory annual cold start resilience test with their largest members every April. SWIFT has routinely shared the results from these tests to all interested members, including smaller members that may be unable or unqualified to participate in such testing, achieving greater transparency for operational resilience standards across the industry entire marketplace and its regulators. Similar, well-designed and broadly based FMI-led proposals for testing protocols, schedules, and participants can serve the larger community of firms in scope for CTP services.

RATIONALE: An example of the high quality that can be gained from examining such processes, third party connectivity mapping is a foundational process that we recommend as a key requirement prior to scenario testing, especially cross-border where are unneeded connections—such as those from testing environments that have not been discontinued/disconnected—can unnecessarily complicate resilience testing processes.

5. (part 1) What are your views on the factors that the supervisory authorities should consider when assessing which third parties to recommend for designation as CTPs?

RESPONSE: Supervisory authorities should base CTP designation on the role those parties play in supporting the critical services that financial sector firms provide. The previously expressed approach described in SS2/21 where a portal is established for vendors could

be a valuable means of means of mapping that would allow financial sector firms to identify critical services, as well as for supervisory authorities to gain assurance that regulators have an accurate understanding of the vendors that support critical services. Alternatively, market reviews that assess the degree of firms' reliance on material FMI services could assist the supervisory authorities in identifying areas of material service concentration for key services involved in cash and securities trading, transfer, and reconciliation activities; exchange and regulatory reporting services (e.g., per ESMA MiFID II/MiFIR requirements); and major cybersecurity and technology infrastructure FMIs, including those services where rapid substitution or service transfers are impractical or impossible.

RATIONALE: Increasingly complex sourcing chain, as noted by the Financial Stability Board, mandate a deeper understanding of the chain's full extent. At minimum, three levels of analysis around designation of CTPs would need to be considered: (1) regulator; (2) industry level needs and resilience standards; and (3) organization level based on unique setting, needs, and risk appetite. While there are very specific rules (e.g. GDPR, DORA, etc.), multiple pieces of legislation are mandating guidance, and these disparate rule sets create more problems than solutions. It is valuable that the Bank of England is focused on cross-border cooperation, as having this in view now will assist with establishing more effective cooperative testing and management processes as the rules emerge.

5. (part 2) Are there any aspects of the criteria discussed above that the supervisory authorities should clarify, develop or omit?

RESPONSE: The PRA might consider how it might develop service-specific impact criteria for the sector.

RATIONALE: It is not within the scope of this response request to make a specific recommendation for the supervisory authorities to resolve or mitigate the various recovery time and other impacts that CTPs might exert on the sector during a catastrophic failure.

5. (part 3) Are there any additional factors that the supervisory authorities should take into account?

RESPONSE: The PRA may consider if there is a framework that could be utilized for sector recovery exercises.

RATIONALE: Sector recovery exercises are of note within the question of resilience planning and minimizing disruptions while firms work to remain within their individual impact tolerance limits.

6. (part 1) 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?

RESPONSE: We recommend the PRA consider establishing a requirement for a designated resilience testing position at an FMI (just as the GDPR mandates the assignment of a Data Protection Officer). We recommend a minimum requirement for setting a baseline, establishing and testing clear lines of communications and feedback. As previously noted, assessments must go to fourth party or beyond (Nth party), in keeping with data privacy regulations, to ensure adequate identification of CTPs. In the event that supervisory authorities intend to provide a sector-wide critical services map, that information should be managed by the regulator in a way that provides visibility without disclosing IP/confidential components of products/services. As noted in our Question 2 response above, this would be expected to influence supplier selection by outsourcers, which could have both positive and negative knock-on impacts.

RATIONALE: Within the current environment, there is still considerable friction against the ability of financial institutions to achieve a clear understanding of concentration risk, materiality, and provision of impact through assessment of third parties. Regulators can provide outsourcers with incremental transparency to know what down chain services represent material functions (that may not be visible to the outsourcer) and what requirements need to be met for resilience standards (e.g., redundant, tested auto-fail replacement services for those functions). The approach in the Discussion Paper to tease out concentration risk by revealing more about the supply chain continuum and all the resulting dependencies is an essential point to reinforce.

6. (part 2) Are there alternative approaches for doing so that could be more effective or pragmatic?

RESPONSE: We recommend establishing what are—for all practical purposes—sector-wide—service-specific impact tolerances. Placing the focus on industry-specific controls would be expected to assist the finance sector in carrying the same weight in the standards set and the controls implemented to manage those standards.

RATIONALE: Examining how other regulators within the UK and in other jurisdictions are successfully achieving strong practices could provide useful structural examples that demonstrate how a high standard is being met for essential products that require regulation for purposes of consumer safety and/or security reasons. Examples include OECD Guidelines on Good Laboratory Practices and the European Medicines Agency's good manufacturing practice (GMP) and Good Distribution Practice (GDP).

7. (part 1) 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?

RESPONSE: A standardized risk management approach should be adopted for all industries that affect the stability of the country's critical infrastructure (Energy, Water, Financial, Communications, and Key Manufacturing).

RATIONALE: Assessing regimes that are disparate is a significant problem across all sectors, including financial. This is especially true for data processing, where geolocation must be disclosed for compliance reasons. Geolocation and encryption constitute two very specific assessment needs and monitoring requirements that are currently difficult for industry participants to meet.

7. (part 2) How could the supervisory authorities improve coordination with other competent authorities and public bodies outside the finance sector?

RESPONSE: The PRA could consider organizations that supervise additional critical infrastructure providers (e.g., Electric, Water, Transportation, Healthcare).

RATIONALE: National and international stakeholders could include insurance, and other critical infrastructure provider regulators across the globe. This body of stakeholders that might serve tangentially to financial sector authorities in the UK includes the G7 Activities Group, US Regulators, European Union regulators, and UK-based critical infrastructure regulators such as the Office of Gas and Electricity (Ofgem).

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?

RESPONSE: It is unclear whether an Nth party alliance with a designated CTP automatically means that the Nth party would be designated as a CTP. In that instance, the question arises of whether the incremental economic burden would be sufficient to prevent that party from supplying that new or expanded service. In addition, there is an alternative risk that firms designated as CTPs may establish a real or perceived barrier relative to smaller or newer marketplace entrants for the same services. Accordingly, all market participants should be encouraged to adhere to and test common resilience standards applicable to both CTPs and non-CTPs. Also, the PRA could also consider the potential impact of a divestiture, merger, or acquisition to potentially stifle competition and thereby accelerate CTP concentration risks if not managed properly.

RATIONALE: Standardizing frameworks would simplify the "requirements to operate" and would establish a clear, defined minimal set of standards that must be met in order to operate when providing a critical service. Third parties would benefit from a clear understanding of resilience requirements and can make an informed decision about whether or not it is economical to enter a market with appropriate infrastructure and processes in place.

9. (part 1) Are the supervisory authorities' potential resilience standards for CTPs clear, comprehensive and proportionate?

RESPONSE: The potential resilience standards are comprehensive and proportionate. The focus is cyber service-based and focuses on the financial implications that may be caused broadly by impacts within this provider type. However, this does not address SaaS and other key suppliers that serve the financial sector.

RATIONALE: As firms individually set impact tolerances for specific services, there will be variations from firm to firm on the basis that impact tolerances are determined on severe, but plausible events. The PRA will ultimately make the determination on what a reasonable impact tolerance will be for each service for the sector as a whole. With reference to proportionality, the supervisory

authorities could consider if the Discussion Paper may target large Cloud Service Providers (CSPs), given their dominance in the market. Reporting requirements could be developed that bear in mind that smaller firms that may be designated as CTPs need proportional standards in order to be able to meet compliance requirements. As an example, the need for auto-fail (go-to) vendors in the event of the shut down or failure of a primary CTP is a basic resilience need. Having stand-by vendors may be more difficult and/or prohibitively costly for smaller providers, though mandating across the industry would help mitigate associated costs.

9. (part 2) Are there any standards that the supervisory authorities could add, clarify, omit or review?

RESPONSE: We recommend potential paths meet generally accepted standards which include: (1) improving transparency; (2) developing specific international standards for multi-tenet environments; and (3) documenting and publishing sector issues and practices.

RATIONALE: Examining existing recognized regulatory standards, rather than attempting to establish a one size fits all approach, would demonstrate where proportional responses may be utilized and how the authority will consider elements of climate-related criteria that are as part of the resilience standards. For example, climate is affecting cooling for nuclear power plants, physical plant and data center risk, and hydro power generation—all of which is deemed within government review and jurisdiction not falling under PRA supervisory authority control. However, this scope is *not* outside cyber resilience in relation to the Discussion Paper's goal for systemic resilience.

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

RESPONSE: Common standards that are based on impact tolerances already utilized by industry should be considered when evaluating CTPs. While many certifications generally add minimal value in this context, an ISAE SOC2 review process could be effectively useful for CTPs.

RATIONALE: Other standards meet the same goals as the Discussion Paper, as they are set by the regulator and require suppliers to meet them and become accredited. Specifically, leveraging ISO 22301:2019 Security and resilience — Business continuity management systems—Requirements, which is being used on an increasing basis within the UK, would be expected to provide the greatest returns for the effort to harmonize regulations and standards.

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

RESPONSE: If successful, this effort could forestall or prevent a catastrophic event for the sector. As mentioned earlier, from a business perspective, operational resilience should be considered as part of a service, and therefore costs for a CTP should be integrated into the costing model. The benefits of such a sector-wide model would ensure a stable and substantially more resilient industry. Technology assistance for the PRA will likely be required (for example, to implement an inventory/register portal) to achieve the level of oversight described in the Discussion Paper; therefore, the PRA should evaluate the need for proportionate funding where required.

RATIONALE: In addition to the implications in the Discussion Paper, such as the insight into concentration risk and the resulting information sharing potential, establishing reasonable (effective, manageable, scalable, and practical), regulations can assure a level playing field for FMIs, firms, and Fintechs across the sector. This regulatory effort would raise the bar for minimum requirements to move firms beyond doing little more than a desktop review to in depth, real world testing. We recognize that implementation of this directive is likely to create an additional cost burden for industry, but if efficiently implemented we expect those costs could be reasonable. Those cost implications may be offset by the leveling of the playing field (in which all parties are mandated to maintain a resilient base that would include auto-fail, go-to vendors) and the need and ability to test regularly and frequently those services to come online without failure. Using DORA as an example, a series of legislative loops are required to achieve a proportional commitment to funding so that the supervisory authorities are properly supported in their efforts.

12. (part 1) What are your views on the potential resilience testing tools for CTPs discussed in this Section?

RESPONSE: While Bank of England CBEST testing may currently be deemed adequate and appropriate, this methodology should be viewed and compared against other testing methodologies with a goal to standardize and adopt common test criterion for use within critical industries in the UK (e.g., Energy, Water, Finance, Key Manufacturing, Transportation, Healthcare). A common test methodology may ensure an efficiency in control creation and testing plans, and therefore reduce cost. We do not have a firm recommendation beyond expanding the gating questions around testing as the process matures.

RATIONALE: With reference to resilience testing to date in the UK, reliable FI-based Red/Blue Team scenario testing requirements have been defined by the Bank of England PRA, which have been deemed appropriate. To test resilience effectively, the primary market of service providers being examined must extend beyond cloud service providers to any third (or Nth) party that provides a critical service within scope for resilience assurance, which requires highly complex, multi-level testing. Such service testing would have to be included in formal agreements with CTPs.

12. (part 2) Are there any additional or alternative [resilience testing] tools that the supervisory authorities could consider applying to CTPs?

RESPONSE: We recommend applying tools that capture changes in resilience indicators over time and also meet the requirements of ISO 22301:2019. These include testing and general BCMS goals that are based on proportionality—a key point in the Discussion Paper—where monitoring; continual, data-driven improvement; and response structures are designed to survive disruption. For some services, a singular point-in-time approach is no longer appropriate. Continuous monitoring for critical services is appropriate.

RATIONALE: *"The outcomes of maintaining a BCMS are shaped by the organization's legal, regulatory, organizational and industry requirements, products and services provided, processes employed, size and structure of the organization, and the requirements of its interested parties…. This document does not include requirements specific to other management systems, though its elements can be aligned or integrated with those of other management systems."* ISO 22301:2019 Security and resilience—Business continuity management systems.

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?

RESPONSE: By tailoring testing regimes and testing cadences to CTPs providing specific material services and leveraging those results with all stakeholders, regulators can achieve desired efficiencies. In addition, to relieve the supervisory authorities and to leverage industry arms, key industry groups should be encouraged to work with their members to establish (or expand) testing criteria, schedules, and participants audited by the supervisory authorities. The Futures Industry Association (FIA), with offices in London, has historically conducted annual industry recovery tests for their major market participants, similar to the SWIFT cold start test.

RATIONALE: Repeatable, transparent controls are essential for quantitative testing. Once industry-level minimum standards for resilience impact tolerances are set, then all stakeholders, including supervisory authorities outside the UK, can operate from the same playbook. Such standardization—and the effective socialization of that standard—would keep stakeholders from working at cross purposes in a way that would be supportive of both regulator and industry goals for resilience.

14. (part 1) In terms of the different potential forms of cyber-resilience testing discussed in this Section, are there any that could be particularly effective for CTPs?

RESPONSE: We have found that the MITRE ATT&CK® Framework sets out a comprehensive test approach and its use could be tailored to the services provided by the CTP to provide a robust framework that is aligned with the PRA's purposes as described in this Discussion Paper.

RATIONALE: Of existing testing and reporting frameworks that can be built upon for cyber-resilience testing, practitioners globally successfully utilize the MITRE ATT&CK® Framework.

14. (part 2) Conversely, are there any that could be particularly difficult to implement in practice or give rise to unintended consequences?

RESPONSE: The need for testing to involve multiple firms, suppliers, and to cross regimes (jurisdictions, borders, regulators) inherently complicates the testing under present circumstances and reinforces the urgent need for harmonizing the approaches to examinations. Test procedures must apply the same level (or greater) of cyber security during testing and to all data and environments that is applied to data across the board (outside testing settings).

RATIONALE: Of note, research has demonstrated that the point of compromise is most often the hybrid (and internal management and level of hygiene) of the platform at the firm level. Outsourcer hygiene in the cloud, which in the shared responsibility model required in cloud, SaaS, and other hybrid environments, is frequently not being managed properly due to technical, time, testing, and other gaps. To the extent that certain concentrations are unavoidable, then it must be incumbent, and regulated as such to be effective, that managing the risk setting also requires standards on how each entity manages its cloud accounts.

15. (part 1) 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?

RESPONSE: Supervisory authorities should share findings and recommendations with organizations that have a clear and immediate need to understand the results of CTP resilience testing exercises. In the context of sector-wide business service failure, there would be notice from the PRA regarding those failures—a power that already exists under that supervisory authority's regulations. Findings should be shared at an appropriate level of detail with designated experts who can interpret the results in a way that will be most useful to the organizations they serve. Note that when the PRA identifies an issue that CTPs would be obliged to communicate directly with their customers (the financial sector firms they serve), as is the typical notification path under existing regulations. Clear roles for reporting should be defined as part of resilience plans (and as noted in our response to Question 6.)

We recommend the PRA consider establishing a requirement for a designated resilience testing position at an FMI, just as the GDPR mandates the assignment of a Data Protection Officer. We recommend that at a minimum for setting a baseline, establishing and testing clear lines of communications and feedback.

If the PRA intends to establish a portal, as suggested in PRA Policy Statement (PS) 7/21, into which firms would be required to populate data on a predetermined set of outsourcing and third party arrangements, our recommendation is that this data: (1) include N^{th} party arrangements as can be reasonably reported (i.e., available to the outsourcer and relevant to critical services); and (2) any insights from that portal be reported/shared with individual actors providing specific services as appropriate to that relationship.

RATIONALE: Of note, the results of testing will provide insight into the weak links in systems, and therefore the regulatory monitoring database that would be created would itself be a ransomware target. Except perhaps in extreme circumstances, it is not appropriate to broadcast resilience testing results. The specific granular detail of test results should be protected from discovery so that cyber criminals cannot act against specific targets with enhanced knowledge that will result in successful attacks. Sanitized results shared with firms would be similar to the SWIFT SIP/Bureau register that shows who meets the standard but without detail. Any necessary details not available to firms would be obtained by the PRA from the CTP directly.

15. (part 2) How could the supervisory authorities balance the need to share this information with relevant firms and FMIs with potential confidentiality or market sensitivity considerations?

RESPONSE: Supervisory authorities could balance the need to share with confidentiality or other market sensitivity considerations by leveraging processes that US regulators currently use when examining and reporting on critical third parties. These processes provide a robust model for sharing results summaries confidentially with existing and perspective customers that has functioned successfully. The regulator could maintain the data trail to the individual outsourcing entities without each entity losing its IP/confidential data that adds value to their individual (or collaborative) end products.

RATIONALE: With the UK chapter of FS-ISAC and CISP (Cyber Incident Sharing Platform) for critical supplier members, some critical infrastructure supplier information sharing takes place at these levels. As security issues arise from the imposition of exposure of pathways and sub-vendors and many organizations reasonably prefer not to divulge the paths that their processes and systems utilize, a significant issue exists for outsourcers and regulators. Where concentrations exist, the question arises as to how the market can be moved to add more players to reduce concentration. From a resilience viewpoint, it would be valuable to encourage growth and more competition in the market. As noted in Basel, Section 34: *"In addition, as financial institutions from different sectors merge and financial conglomerates evolve, the potential for new types of concentrations arises. When evaluating proposed mergers or expansions, supervisors should take into account management plans to manage material risk concentrations at a group-wide level."* For example, insurance companies are heavily dependent on certain critical third parties (as acknowledged in the Discussion Paper findings) and, therefore, there exists a need to encourage a broader base or a different infrastructure that does not rely on the same pathways.

15. (part 3) Could a rating system along the lines of the Uniform Rating System for Information Technology (URSIT) system used by the FFIEC in the US promote clarity and consistency in supervisory authorities' assessments?

RESPONSE: Rating systems for individual providers could be effective.

RATIONALE: Ostensibly, any rating system would be viewed through the lens that the supervisory authority is able to realize through analysis and mapping of targeted data.

16. (part 1) Could a set of global, minimum resilience standards for CTPs be helpful?

RESPONSE: A common set of global minimum resilience standards would be very beneficial. Standardization would allow for efficiencies and the ability to leverage reporting, testing, etc. across multiple sectors and countries.

RATIONALE: Unified standards are a laudable goal. Leveraging existing ISO Resilience Standards, including ISO 22301:2019, 22316, and others would provide a solid foundation for setting global minimum resilience standards.

16. (part 2) If so, what areas should these standards cover?

RESPONSE: When determining what areas these standards should cover, we recommend that more attention be accorded the requirements imposed relative to the existing and emerging challenges that companies already face in meeting increasing requirements. Leveraging existing ISO Resilience Standards, including ISO 22301:2019, 22316, and others would provide a solid foundation for setting global minimum resilience standards.

RATIONALE: Key cross sector criteria examples from DORA's specific objectives include: "*Address ICT risks and strengthen digital resilience; Streamline ICT-incident reporting; Provide access for supervisors to ICT incident-related information; Ensure assessment of preventive and resilience measures; Facilitate cross-border acceptance of testing results; Govern the monitoring of ICT third-party providers; Oversee critical ICT third-party providers; and Exchange threat intelligence*."

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?

RESPONSE: Developing a set of agreed upon resilience testing and reporting requirements is key to cross-border collaboration. To enable resilience testing of CTPs in a coordinated manner, the authority needs to examine: (1) mechanisms that can identify scenarios that limit data availability; (2) effects of such limits on a processing activity, (3) preliminary metrics to diagnose these "shared responsibility model or management" risks; and (4) strategies to reduce exposure stemming from concentration risk.

RATIONALE: One key area that is consistent across standards and jurisdictions is the knowledge of where data are stored and ways in which storing protected data are managed. Shared responsibility (as indicated in our response to Question # 14) would also dictate the need to establish default deployments for IaaS, PaaS, and other network/cloud based services.

18. (part 1) What forms of testing could be most appropriate (ie sector-wide exercises, TPLT or other forms)?

RESPONSE: Regulators have the ability to incentivize these activities and therefore can impact the future resilience of the sector through this process. It would be valuable to build on forms of cross border testing such as Quantum Dawn and G7 Activities Group, as these are increasingly applied for complex scenario testing and have already been taking place on a voluntary basis. Because financial and insurance firms, supervisors, and third parties are already involved in these exercises, advancing this methodology would facilitate implementation of the upcoming advisory. As a first step, one agency that might be able to bring regulators together worldwide is the Financial Stability Board (BCBS or an equivalent organization of like-minded supervisors) under one umbrella. Continuous monitoring is widely accepted in today's complex and dynamic environment. Supervisory authorities should have a specific focus on testing the effectiveness of CTPs' continuous monitoring programs, as well the effectiveness of continuous monitoring programs sector-wide.

RATIONALE: The need exists for these types of exercises to be real-world, severe, and plausible, including ransomware and the ability of a third or Nth party to respond and/or recover in the event of systemic failure(s). Best practices include workbooks being provided before the exercise to optimize the involvement of the parties participating while the exercise is taking place. The lack of this type of preparation has become an overwhelming problem during testing exercises. Firms also need to have incentives to participate and understand why war room level activities are necessary. There is a lack of experience in the skills pipeline globally to test and respond effectively, including in the UK. Firms need to understand that this is a significant gap. The market can also support this effort as it is a compelling business case for clients to know that this level of participation is being carried out, and therefore strengthening public confidence in the sector.

The Financial Stability Board compiled a survey of third party supervisory regulatory regimes around the world, which is reflected in the need and understanding among regulators that rules harmonization across jurisdictions and sectors in in the best interest of regulators and regulated industry members (BCBS, Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper). Alignment needs to be achieved with reference to laws across jurisdictions and with cross industry regimes outside the financial sector to be effective and take into account cross talk as opposed to cross border regimes (e.g., APAC/China, regional, as well as sector requirements). Where similar services are being provided to financial organizations that are already being managed for bodies outside financial sector, there needs to be practical guidance so that organizations do not fall into conflict with GDPR and other international versus domestic bodies. Benefits can be realized sector-wide when regulators spend targeted time with their industry counterparts in order to determine how best to manage coordination. Any other approach will continue to yield block by region, geopolitical/economic base, and other dividing criteria.

18. (part 2) Are there any practical challenges in these cross-border exercises which the supervisory authorities should anticipate and manage?

RESPONSE: A key challenge is dealing with environments where regulators may not wish to share potentially confidential test results with other regulators on a universal basis. In addition, a cross-border regulator may lack jurisdiction or direct authority to regulate or otherwise view test results for a CTP or related Nth party operating in their geographic area. Having a trusted international agency (e.g., FSB or BCBS) or an equivalent organization of supervisors worldwide coming together under one umbrella would be a major step towards ensuring a successful effort and appropriate forms of information sharing.

RATIONALE: Cross jurisdiction evaluation of critical third parties without regulatory harmonization and/or testing reciprocity could result in conflicts that may be difficult to resolve. Whatever steps the PRA can take to achieve harmonization with EU and other regulators should be given high priority.

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?

RESPONSE: It is worth noting that collaboration and information sharing can serve as levers that allow regulators to encourage the development of robust resilience requirements around CTPs.

RATIONALE: A gating step to improving international regulatory and supervisory coordination in relation to the risks posed by CTPs is for regulators to achieve an acceptable degree of harmonization in evaluating, testing, and monitoring resilience risks. Without it, weaknesses may be created in markets that could potentially affect resilience in unexpected ways. The harmony would come from a data-driven process of identifying financial sector market risks (based on data collected and analyzed) to show those stress points and the implications of those points of risk, including concentration risk. Communications have to improve between the financial sector and supervisory authorities so that the joint goal is always clear to all stakeholders—protecting the larger market stability within a given jurisdiction.

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 (subject to certain conditions)?

RESPONSE: Resilience tests, sector-wide exercises, and other oversight activities conducted by responsible entities in other jurisdictions are appropriate as long as all aspects of testing exercises and reporting meet UK and globally accepted regulatory standards. Harmonized testing across jurisdictions is essential to maximize efficiency in assurance processes.

RATIONALE: Any approach to supervisory authority involvement would be most effective if it is applied sector-wide and takes into account: (1) what can be outsourced (i.e., is already taking place in various jurisdictions globally); and (2) development of widely accepted reporting formats. That would allow for a 'do it once and spread the results' approach that fosters benefits and reduces compliance costs and fatigue. This approach requires that regulators be motivated to set the goal to establish and maintain formal agreements across international boundaries where rigor of standards and reporting metrics are harmonized.

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?

RESPONSE: Cross-sector industries that present critical services to the UK such as Energy, Finance, Water, Transportation, Healthcare, and Key Manufacturing should be considered for cross-sector standardized controls.

RATIONALE: One standard across documentation will: (1) bring down costs; (2) increase efficiency; and (3) can improve response time. To minimize the governance cost, standardization will allow adoption once and efficient monitoring and testing of a robust operational resilience program that can address the needs of multiple critical industries at once. This program should be in a position to be shared for all users of the CTP provided service, beyond the financial sector where impacts may be exerted on other critical industries.