Shared Assessments
PRA CP26 23 Response

Date: March 15, 2024

To: The Recovery, Resolution and Resilience Team
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA

Email: CP26_23@bankofengland.co.uk

From: Andrew Moyad, CEO, Shared Assessments LLC

Subject: CP26/23 – Operational resilience: Critical third parties to the UK financial sector – Bank of England Prudential Regulation Authority and the Financial Conduct Authority (FCA) Joint Consultation Paper 26/23 | FCA consultation paper 23/30

Shared Assessments appreciates the opportunity to submit comments to the Bank of England Prudential Regulation Authority and the Financial Conduct Authority joint Consultation Paper on Operational resilience: Critical third parties to the UK financial sector.

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 that defines best practices, develops tools, and conducts pace setting research. Our 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 organization and its members, thank you for accepting the following response to Operational Resilience Consultation Paper CP 26/23.

Shared Assessments
PRA CP26 23 Response

Shared Assessments
PRA CP26 23 Response

Question	Response and Rationale
*1. Do you have any comments on the regulators' **definitions of key terms and concepts** outlined in Chapter 2 of the draft supervisory statement? Are there key terms or definitions the regulators could clarify or additional definitions to be included?*	These definitions could serve as the basis for rationalizing definitions and other language (such as the definition of incident) across jurisdictions and agencies (NIST, ISO, PRA, EBA, other regulators and standards organizations). Rationalization of these terms across jurisdictions should be a high priority. Will the regulators disclose the general impact criteria they use to designate critical third parties? The provision should cover all operating capabilities for non-critical and critical services because the risks posed across the CTP's service line cannot be effectively segmented. It would be useful for the regulator to identify in general terms some of the criteria that might be applied in the definition in section 2.19 "Where data alone is insufficient to identify a CTP, the regulators will use judgement"?
*2. Do you have any comments on the regulators' **overall approach to the oversight regime for CTPs** outlined in Chapter 3 of the draft supervisory statement?*	The tasks involved in identification and mapping to meet the regulator's overall approach will be critical, but difficult, in long supply chains. The practicality of achieving these mapping requirements will improve over time. As regulatory mapping capabilities mature, regulators may be able to play a material role in helping both financial institutions and CTPs map critical supplier components in their supply chains. Regulators should set more specific expectations about the broad types of data CTPs will be required to provide, including supply chain-specific mappings. The proposal suggests (Section 2.2.6) "…that, over time, firm/FMI data will become the main source of data to support the identification of potential CTPs." One-off solutions employed to mitigate otherwise untenable risks may at times create another level of complexity for regulators. Therefore, it is critical that regulators capture as much supply chain information from FMIs as possible. In fact, over time regulators may be able to inform FMI understanding of their own complex supply chains. The previously expressed approach described in SS2/21 where a portal could be established to track outsourcing inventories in near real-time 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. This near-real-time portal represents a technique that could serve as a model in other jurisdictions. Please refer to our response in Question 17 regarding protection of confidential and sensitive data. The element of the regulator's approach to testing is discussed in our response to Question 13.
*3. Do you have any comments on the regulators' **proposed Fundamental Rules**? Should the regulators add, clarify, or remove any of these Rules, or any of the*	The Fundamental rules serve as a good high-level base of expectations. CTP Fundamental Rule 6 states "A CTP must deal with the regulators in an open and co-operative way, and disclose to the regulators appropriately anything relating to the CTP of which they would reasonably expect notice." Final regulations should provide robust examples about the types of information that would likely be included in data collection.

Question	Response and Rationale
terms used in them, eg 'prudent', 'responsibly'?.	The language in CP 26-23 enabling assessments of CTPs is similar at a high level to the Bank Service Company Act (12 USC Section 1867, Regulation and Examination of Bank Service Companies), which notes the federal banking regulatory agencies can make examination of service companies that serve a regulated entity, "subject to the provision of Section 1818 as if the service company were an insured bank" …."to the same extent as if the service were being provided by the bank on its own premises…" Having multi-jurisdictional regulatory authority to assess critical third parties who often have wide geographical footprints is helpful by itself, and having similar regulatory regimes across jurisdictions creates common expectations to the benefit of all parties.
*4. Do you have any comments on the regulators' **proposal for the Fundamental Rules to apply to all services a CTP** provides to firms or FMIs?*	This provision for fundamental rules to apply to all services a CTP provides to firms or FMIs is essential. The provision should cover all operating capabilities for non-critical and critical services because the risks posed across the CTP's service line cannot be effectively segmented. To the extent that this provision supports continuity and reputation of the financial sector, a lack of adherence to the fundamental rules across all of a CTP's services could impact material services being provided to firms or FMIs. Information needs to be available to identify single source providers and groups of providers that escalate risk to the point of failure could be catastrophic to the system (such as SWIFT or Euroclear).
*5. Do you have any comments on the regulators' **proposed Operational Risk and Resilience Requirements**? In particular, should the regulators add or remove any of these Requirements?*	We agree that a minimum standard of resilience should be laid out and guidance/requirements published for CTPs to follow in respect to CTP services, whether critical or not. Regulators may be able to help critical third parties identify Nth parties that are not readily visible in their supply chains. 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 in an organization that provides a critical service. The provision should cover all operating capabilities for non-critical and critical services because the risks posed across the CTP's service line cannot be effectively segmented. Third parties would benefit from a clear understanding of requirements and therefore can make an informed decision about whether or not it is economical to enter a market with appropriate infrastructure and processes in place. All market participants should be encouraged to adhere to and test common resilience standards applicable to both CTPs and non-CTPs. Also, the regulator should consider the possible impact of a divestiture, merger, or acquisition that may accelerate CTP concentration risks if not managed properly. Please provide more clarity around the basis for determining the intervals between regulatory examinations (for both firms/FMIs and CTPs) and what specific events, if any, might trigger an off-schedule examination. Of note, it is unclear if the regulator will exercise the right to examine at scheduled intervals and against specific thresholds (e.g., materiality).
*6. Are there any aspects of **specific requirements that the regulators should clarify**, elaborate on, or reconsider?*	We do not have any points for reconsideration. We recognize that the Identification requirement in section 5.2 mandates that a CTP identify and document its material services. Additionally, the regulator acknowledges in section 2.24 that the regulators are further responsible for identifying what services are material and therefore critical.

Question	Response and Rationale
7. Do you have any comments on the regulators' proposal for the Operational Risk and Resilience ***Requirements to apply to a CTP's material services only****?*	Ideally, we would like to see these rules applied across all services that a CTP provides. Lax protocols in services deemed 'irrelevant" to the designation as a CTP could ultimately cause vulnerabilities that may compromise the critical service. Where a CTP's services might not fit the definition of material services, a lack of adherence to the fundamental rules by those parties could potentially impact material services. Nth parties across the supply chain are not covered in detail in this Consultation Paper. How will the regulators use the information from CTPs to help manage supply chain elements or other vulnerabilities that are not readily visible to outsourcers?
8. Do you have any comments on the regulators' proposal to ***require CTPs to (separately) notify their firm/FMI customers and the regulators of relevant incidents****?*	The only reference to notifications in that document is in section 8.1.12 of the sourcebook indicating a firm should notify the FCA when it intends to rely on a third party for the performance of critical or important functions (Section 7.1 indicates that the proposed notification requirements in Chapter 8 of the Critical Third Parties sourcebook in the FCA handbook). A carefully secured centralized repository or clearinghouse of incident notifications could ease the burden on CTPs and potentially provide their firm/FMI customers and regulators with notification of the incident earlier than those parties would otherwise receive.
9. Do you have any comments on the regulators' ***definition of 'relevant incident'****?*	The definition of 'relevant incident' is consistent with similar definitions from other UK and US authoritative sources. It is also consistent with the benefits of nomenclature harmonization across regulators and most standards organizations.
10. Do you have any comments on the regulators' proposals to ***require CTPs to submit initial, intermediate, and final incident notifications*** *to firms and FMIs and the regulators?*	Conceptually, this approach appears fair and reasonable. A minimal prudential standard is being set that can help protect the sector. While the approach is conceptually sound, it should be noted that the regulation establishes a floor and ceiling for providers that may not always meet best practice guidance for due diligence that would reveal potential impacts or gaps/controls outside of the floor/ceiling set by the regulation. It is worth considering that if this becomes rule in UK, contracts might need to be written in such a way that ensures continuing dialogue outside of the minimum point-in-time of the notification process that make it clear that the conversation between the CTP and the client could be an ongoing dialogue. The process could provide a consistent model for other jurisdictions (globally) because the three stages represent a natural progression for notification processes. Regulators could periodically review and adjust notification policies as technology or incident response needs evolve.
11. Do you have any comments on the regulators' proposals regarding ***what information should be included at each stage*** *(initial, intermediate, or final) of notification?*	The notification requirement proposals outlined in sections 8.2-8.4 of the document appear reasonable. Please consider whether it may be of benefit to the regulator might to be provided with an additional "pre-incident determination notification" from the CTP that could contain fewer requirements in order to facilitate earliest warning from a suspected incident when a defined set of triggers occurs. Recognizing that this step would yield increased false positive notifications, would the burden of false positives be offset by the benefits of early notification? Please note that Point 2 of section 8.4.1 under Final Notification conflicts with the assumption that this notification occurs once the incident has been resolved ("… a description of any remedial actions the critical third party has or is planning to put in place and an estimated timeline for the completion of those remedial actions;…").

Question	Response and Rationale
*12. What are your views on having a **standardised incident notification template**?*	A standardized notification template would provide efficiencies for all parties (outsourcers, CTPs, and regulators). An additional benefit of a standardized template would be the likelihood of collecting information in a consistent manner that can be more easily analyzed. Standardization should also reduce the cost of compliance and enable smaller institutions who are customers of CTPs to receive the same data as larger institutions with larger spend with a CTP.
*13. Do you have any comments on the regulators' proposed rules and expectations in relation to **information gathering and testing**?*	The provision (section 6.15) to allow the CTP or the regulator under s166(3) FSMA is reasonable. 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 Nth 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. 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. The Financial Stability Board could be an agent to develop multi-jurisdictional quantitative testing expectations. 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. 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 participate in exercises led 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.
*14. What are your views on whether the regulators should include **additional mandatory forms of regular testing for CTPs**?*	We do not see a reason to include additional mandatory forms of testing above what is already proposed. Please note, forensic testing guidelines would be valuable in the final rule. We have additional responses regarding testing in our response to Question 13.
*15. Do you have any comments on the regulators' proposals to require **CTPs to share certain information with firms and FMIs**?*	The sharing proposal described in Section 6.23 is appropriate.

Question	Response and Rationale
*16. Would the information the regulators propose to require CTPs to share **benefit firms' and FMIs' own operational resilience and third-party risk management**?*	Yes, it would be beneficial for firms and FMIs to receive this information. Assuming that regulators would be able to share select collected information, financial institutions would be better able to protect themselves, especially through identification of the presence of critical third parties buried in supply chains and by extension the sector.
*17. Do the regulators' proposals **balance the advantages** of sharing relevant information with firms and FMIs **against potential confidentiality or sensitivity considerations** for CTPs? Are there any additional safeguards that the regulators could consider to protect confidential or sensitive information?*	Obviously protecting both information and insights garnered from the collective knowledge is critically important. Now that NIST is releasing recommendations to safeguard information in the coming quantum computing environment, and firms (e.g., Apple) are beginning to adopt those recommendations in the marketplace, this collective information and the insights garnered from it should be quantum-protected and otherwise protected against other emerging attack vectors. Supervisory authorities should share findings and recommendations only 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. Regulatory 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 outsourcers. Note that when the PRA identifies an issue, CTPs would be obligated to communicate directly with their customers (the financial sector firms they serve) and other impacted firms, 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 Nth 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 as appropriate to that relationship.
*18. Do you have any comments on the regulators' proposals to restrict CTPs from indicating, for marketing purposes, that **designation implies regulatory endorsement or that its services are superior**?*	The proposals appear reasonable. No other measures come to mind. We do recommend regulators consider that designation could have unanticipated impacts that may reduce competition for a certain set of services, as noted in our response to Question 19 below.

Question	Response and Rationale
*19. Do you anticipate any other **unintended consequences from the designation** of CTPs? Are any further requirements necessary to avoid these unintended consequences?*	The possibility exists that third parties may avoid providing certain services and/or contracting with firms and FMIs that would push them toward CTP designation and require them to comply with stricter CTP requirements. There is an alternative risk that firms designated as CTPs, and possibly the CTP's Nth parties, may establish a real or perceived barrier relative to smaller or newer marketplace entrants for the same services. If the provider is at a tipping point for designation, they may think twice about taking on additional commitments that might push them into the CTP designation.
*20. Do you have any **comments on the cost-benefit analysis**? Do you have any comments on the regulators' proposals to restrict CTPs from indicating for marketing purposes that designation implies regulatory endorsement or that its services are superior? Are there any **other measures** which the regulators could consider **to mitigate potential, unintended adverse impacts on competition** among third party service providers as a result of the designation of CTPs?*	The cost-benefit analysis at sections 1.39-1.43 and Appendix 6 appears to reasonably capture the initial and ongoing costs of the proposed rules. However, the cost-benefit analysis does not identify benefits to CTPs, which could have the unintended effect of dissuading third parties from providing services and taking on firms and FMIs that may designate them as a CTP. The benefits described are focused on the sector outsourcers (users). Benefits need to be clearly identified for designated CTPs. Positive impacts to the CTP may result through incrementally improved due diligence from parties in the supply chain other than the CTP itself. Regulators will lead testing on CTPs that can yield insight into control effectiveness deltas. When those deltas are closed, the CTPs and their customers benefit. While we recognize that implementation of this directive is likely to create an additional cost burden for industry, if efficiently implemented we expect those costs could be reasonable and the benefits important. Those cost implications may be offset by the leveling of the playing field (in which all parties are mandated to maintain a resilient base of previously vetted 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 could be required to achieve a proportional commitment to funding so that the supervisory authorities are properly supported in their efforts. In the future, cross-jurisdictional process standardization will likely provide industry-wide economic efficiency.