Facilitating a better future
lmalloyds.com

Lloyd's Market Association
Suite 426 Gallery 4
One Lime Street
London EC3M 7DQ
T. 020 7327 3333

16 December 2022

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

Email: DP3_22@bankofengland.co.uk

Dear Sir/Madam

LMA response to DP3/22 – Operational resilience: Critical third parties to the UK financial sector

The Lloyd's Market Association (LMA) represents the 52 managing agents at Lloyd's, with 93 active syndicates underwriting in the market, and also the three members' agents which act for third party capital. Managing agents are "dual regulated" firms by the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) and members' agents are regulated by the FCA. For 2021, premium capacity is in excess of £30 billion.

We welcome the opportunity to respond to the Discussion Paper

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

1. We agree that increased reliance on third parties which create significant levels of concentration within the financial sector may have an impact on the PRA's and FCA's supervisory objectives. However, as the Discussion Paper notes, regulated firms do not generally have sufficient information on third parties' exposures to other parts of the financial industry and therefore a central oversight mechanism is necessary.

2. We also note that certain firms and their products are ubiquitous, and therefore unsubstitutable in an operational context. For instance, failure of Microsoft 365 Azure services might have the ability to halt business operations where the only 'plan B' available to firms would be to wait until the services come back online or maintain unreasonably costly back-up services. The oversight framework for material services provided by critical third parties should consider such scenarios.

3. Whilst the Discussion Paper mentions cloud service providers and IT services as an example of potential critical third parties (CTPs), it is unclear what the scope of the new framework would be and how far it would reach into the non-technology world. The regulators need to consider this matter and share their thinking with industry so that all parties can evaluate the impact and workability of proposals.

4. Also of importance is the need for regulators to communicate clearly a CTPs level of resilience (for the service or services purchased) to current and future customers in such a way that the firm can, on an ongoing basis, fully understand the level of risk within their supply chain.

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

5. We agree with the regulators' assessment of the limitations of the current regulatory framework. We feel that, to maximise effectiveness, the new framework needs to be integrated with the operational resilience frameworks of regulated firms. As such, there needs to be a mechanism for ensuring that regulated firms receive sufficient information from the regulators to allow them to gain comfort regarding the use of those CTPs.

6. The regulators need to consider and then set out:

    a) The extent to which the regulatory framework will reduce the due diligence obligations of regulated firms.
    b) How the regulators will use any powers to direct CTPs to remediate issues.
    c) What the regulators' expectations of firms will be.
    d) How the regulator will use any enforcement powers.
    e) How the use of any such enforcement powers might affect the ongoing viability of firms' operations.

    We feel considerations of the above is crucial as individual firms are increasingly unable to exert meaningful pressure on CTPs themselves.

7. We would note that many CTPs are likely to provide various services to firms and the regulators need to consider the likely granularity of their oversight and regulation. Would the regulators expect CTPs' material services to include all services they offer to firms?

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

8. Whilst the Discussion Paper sets out the areas that minimum resilience standards could potentially cover, further detail is needed to provide a proper assessment of their appropriateness.

9. We would ask how the regulators see the framework operating in practice.

    a) Will there be a recognised standard that CTPs need to meet (akin to ISO, etc.)?
    b) Who will be responsible for testing?
    c) How will results be promulgated across industry?
    d) How can the regulators avoid a minimum standard resulting in a "race to the bottom"?

10. We think it is critical that the results of testing are published in order to ensure transparency for the firms who carry the risk. Such reporting should be standardised and, if performed by the CTP, audited by an independent third party.

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

operational resilience framework? Are there alternative approaches the supervisory authorities should consider?

11. We fully support the proposal to align measures for CTPs with the existing operational resilience framework as this would help ensure that CTPs operate within the same parameters as regulated firms and that the latter can readily integrate those material services into their own operational resilience frameworks. We suggest a taxonomy of material services/IBSs would be a useful tool in allowing firms to monitor CTPs and assess concentration risk.

12. Assuming the framework for CTPs aligns with operational resilience frameworks for firms, we would ask how the regulators intend to measure and report Impact Tolerances. Will there be an expectation that CTPs meet the Impact Tolerances of the firms to whom they provide services, or will it be for firms to check that the CTPs' Impact Tolerances align with their own?

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

13. We agree with the proposed criteria for determining recommendation of CTPs. However, we would note that robust risk management could include other considerations, e.g. geographical concentration, political environment, etc.

14 In addition, to provide for a holistic approach, the regulators would need to "look through" the value chain to determine service providers which could present a systemic risk to the financial services. However, that approach needs to be balanced with the need for a manageable framework.

15 The suggestion in 14 above would be important in terms of the scope of any regulatory framework as, ultimately, firms and CTPs will be dependent on services which are inherently unsubstitutable, e.g. power network providers and water companies, etc. Our assumption is that such service providers which provide the foundations for all business will be out of scope.

16. Regarding the practicalities of the designation process, the regulators will need to consider and communicate:

    a) How often the list of CTPs will be reviewed?
    b) Lead in times for inclusion of a new CTP to the list.
    c) How a CTP could/would be removed from the list.

17. We suggest that the regulators explore the possibility of allowing service providers to 'opt-in' to designation as a CTP in order to allow them to assess for themselves whether any potential competitive advantages of being designated outweigh the potential costs. Alternatively, the regulators could consider a 'certification' regime in which service providers could be assessed to provide the same level of resilience as a CTP. These options could minimise concentration risk and any reduction in competition.

Question 6. What are your views on the supervisory authorities' potential approach for assessing concentration, materiality and potential impact in the provision of third party

services to firms and FMIs? Are there alternative approaches for doing so that could be more effective or pragmatic?

18. We support the regulators' approach to assessing third parties' concentration, materiality and potential impact in the provision of their services. In relation to concentration, we also agree that market share appears an appropriate measure. However, in line with our response above, we suggest that the regulators need to provide further information on how this will be done in practice, and a view about what the regulator position will be if one CTP poses too high a concentration risk.

19. The "Potential factors relevant to CTP designation" table on page 34 of the DP is useful. However, further consideration of the criteria of the factors in a similar way to that for concentration, along with some worked examples of the interplay, would be helpful.

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

20. We support the regulators' intention to seek cooperation with regulators outside the financial services industry and, indeed, outside the UK. We consider it important for the critical third-party oversight frameworks to ensure consistency in definitions and requirements to the extent possible to avoid any unnecessary duplication of oversight activity. Regulators should seek efficiencies where possible and avoid scenarios where third parties have to respond to multiple regulatory queries of broadly similar nature which could be managed through better supervisory coordination.

21. We note the work of the Digital Regulation Cooperation Forum which seeks to ensure greater coordination on online regulatory matters. Similar cooperation mechanisms can be created for the oversight of material services provided by critical third parties and to address the cross-sectoral issues that will inevitably arise in this context.

22. There are several UK agencies/initiatives which could be coordinated with including the National Risk Register, the Uptime Institute for data centres, the National Cyber Security Centre (NSC) and the Centre for the Protection of National Infrastructure (CPNI).

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

23. We agree with the concern stated in the Discussion Paper that the new framework could result in unintended consequences, such as changes in the structure and allocation of the third party services market. The risk is regulatory arbitrage where some providers cease providing certain services to avoid being classed as a CTP. This could reduce competition, further increasing concentration risk.

24. The regulators should therefore seek to understand the concerns of potential critical third parties and potential commercial impacts. The proportionality principle should then be applied rigorously to minimise unnecessary expense. The regulators will then need to carefully monitor the impact of the new rules in the early stages of the implementation to ensure that they can respond effectively to any detrimental consequences of the requirements.

25. New regulatory requirements for CTPs parties are likely to require increased compliance costs. Those costs will inevitably be passed on to firms who will also bear any increased supervisory costs for the regulators. Ultimately, the new regulatory framework will result in increased costs for consumers.

26. We would advocate a pilot scheme, overseen by an independent steering committee, to identify risks and costs and assess potential benefits ahead of any full-scale roll-out.

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

27. The Discussion Paper has, understandably, been written from a regulator's perspective, rather than that of a CTP's customers, although it is those customers who carry the day-to-day risks. All relevant information should be made available to firms during the RFP/evaluation phase and during the assurance activities undertaken by a potential or actual customer. In terms of the resilience standards:

    a) During the identify phase CTPs should be made to clearly document the IBSs their customers are managing and the CTP's services which support those IBSs. i.e. there should be a documented direct link between IBSs and the supplier's services to demonstrate that the CTPs understand the dependency.
    b) The CTP should document the link between the customer's recovery time object (RTO), Recovery Point objective (RPO)s, and maximum service outage (MSO) and how these are being contractually met by the CTP.
    c) There are three comparisons - the customer's internal RTO, RPO and impact tolerance, the contracted RTO, RPO and MSO, and the RTO, RPO and MSO delivered during incidents and tests. All these should be published annually within a standardised report and distributed to the CTPs customers, customers in pre-contractual negotiations and the regulators.
    d) A reporting phase should be introduced whereby each of the services are documented and reported on so that customers can accurately understand the level of resilience and therefore risk associated with the service they have purchased. The report should be published at least annually. The report should include test results and the impact of any incidents during the previous 12 months, together with any planned remediation and resulting proposed changes.

28. The potential resilience standards set out in Table C on page 39 are high-level and more detail is required in order to provide effective feedback.

29. As per our response to Question 16, we also encourage regulators to seek the harmonisation of international standards to enable a more consistent international approach to the oversight of services provided by CTPs, in particular such areas as resilience testing and incident reporting frameworks.

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

30. Regulated firms already take account of third parties' relevant certifications as they offer reassurance about the level of internal controls and safeguards maintained by those parties. We would support utilisation of ISO, Kite Mark, or other such recognised standards.

31. Furthermore, we would encourage the regulators to certification schemes any gaps or discrepancies to allow the schemes the opportunity to make appropriate adjustments.

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

32. As previously stated, we anticipate that bringing material services provided by CTPs within the regulatory perimeter will likely increase compliance costs for affected businesses. It is difficult to predict how the services market will respond to this, but it may create additional barriers to entry/growth for smaller firms when they increase their operations and face designation as a CTP. Similarly, firms dealing with non-critical third parties might apply higher standards to such firms in line with their engagement with CTPs. Such barriers could affect diversity of the supply chain which would be contrary to regulators' objectives.

33. The new framework, if implemented appropriately, could bring certain benefits, such as providing a consistent set of requirements across both firms and their CTPs. Creating a single set of regulatory expectations should support the interaction between firms and their service providers and facilitate a more efficient onboarding and oversight process.

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

34. We support the regulators' use of resilience testing tools as this enables practical understanding of third parties' vulnerabilities. In this context, scenario testing is the most widely used option, but levels of sophistication vary with cyber scenario testing perhaps at the most advanced stage of development and implementation.

35. The Discussion Paper refers to sector-wide exercises and we agree that they can provide valuable lessons for the entire finance sector. CTPs and regulated firms already undertake their own testing; sector-wide exercises would build on that and allow for independent verification of the results. We note, however, that the framework for sector-wide testing requires further work in the context of insurance. We further note that the Discussion Paper makes no mention of testing disaster recovery plans.

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

36. Engagement will be key. Regulators and/or CTPs could make use of accounting/auditing firms who have substantial experience of testing control frameworks. As previously stated, we think transparency is of the utmost importance and we reiterate the need for all testing to be available to firms.

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

37. We agree with the limitations of cyber resilience testing set out in paragraph 6.27 of the Discussion Paper.

38. We agree with the regulators' proposals to require relevant CTPs to support firms' cyber resilience tests and also conduct their own resilience testing. We also agree that CBEST is a

useful tool, although extremely resource intensive. As such, to maintain the principle of proportionality, a flexible approach to testing should be adopted.

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

39. We feel that an overall score for a CTP would unlikely have sufficient granularity to allow customers to accurately understand its level of resilience and therefore the level of risk associated with that particular service.

40. CTPs should have to provide an annual report in a standard format to the regulators and their actual and customers in precontractual negotiations. The report should detail the level of resilience of each of the services provided so that the customer can understand the level of risk they are taking by contracting with the supplier. An aggregate score for a CTP with more than one product and one method of delivery would have little value.

41. We agree that potential confidentiality and market sensitivity considerations need to be taken into account when sharing information. Standardisation of the feedback format could be one way to address this as such an approach could help ensure that only pertinent information at the appropriate level is captured.

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

42. We support the idea of global resilience standards for CTPs, particularly for groups with global networks, as this would avoid conflicting requirements and expectations. However, we feel a global solution will be difficult to achieve and, due to the speed of progress, quickly become redundant.

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

43. We feel a standardised reporting format would be beneficial, together with a common approach to "severe but plausible" scenarios and associated scenario tests, built around a common taxonomy.

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

44. We agree that TLPT would likely be an appropriate form of testing. We would reiterate that resilience testing is a resource-intensive undertaking and effective planning would be essential to avoid an unnecessary burden through multiple exercises undertaken in different jurisdictions.

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

45. Formalising co-operation between jurisdictions will be an essential step towards facilitating success in international oversight efforts. This could be achieved through creating new or adjusting existing memoranda of understanding between regulatory authorities to capture elements, such as exchange of information, allocation of responsibilities and joint regulatory work in respect of critical third parties.

46. The Financial Stability Board (FSB) may represent an appropriate forum for collaboration with respect to certain large service providers given some third parties will be critical to the financial sector as a whole at a global level, rather than individual sub-sectors or geographies. Other areas to explore include inter-governmental treaty arrangements and co-ordination with/through the World Economic Forum risk reporting process.

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

47. Reliance on the oversight activities undertaken by overseas supervisory authorities needs to be supported by the internationally recognised and implemented standards that would provide certainty to all parties that regulators operate within a certain set of parameters. In such a scenario, regulators would need to reach 'equivalence' determinations in relation to other jurisdictions which would enable reliance on the work undertaken there.

48. One mechanism to achieve this objective would be for the IAIS to develop a new Insurance Core Principle that captures the necessary features of the CTP oversight regime. Adherence to the IAIS Insurance Core Principles is regularly tested through the IMF Financial Sector Assessment Programme which would give participating jurisdictions assurance that they can rely on the work undertaken in the relevant jurisdictions.

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

49. We would encourage cross-sectoral cooperation and feel it is essential across fuel, defence and intelligence where CTPs may be most critical.

Please do not hesitate to contact me should you require any additional information.

Yours faithfully

Matt Wood

On behalf of LMA Operational Resilience Committee
matt.wood@lmalloyds.com
Tel: 020 3307 3934