FIA response to BoE, FCA, PRA CP - Operational resilience: Critical third parties to the UK financial sector

Introduction

FIA supports the proposed approach, which provides for regulators to build on and complement operational resilience frameworks for firms and FMIs. FIA members also support the proposal for oversight of Critical Third Parties (CTPs) to be as interoperable as reasonably practicable with similar existing and future regimes. Furthermore, FIA members support the proposals to promote regulatory and supervisory interoperability.

Question 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?

In general, FIA members believe the proposed approach of considering each third-party and the different services they provide based on inputs/data received from their users to be appropriate.

Key entities and persons – Critical Third Parties

FIA believes intra-group services companies within a regulated financial group should be excluded from CTP designation on the basis that these firms typically do not provide services to any entities outside of their group and their interests are aligned with the other entities within the group to which they provide services in terms of effectively managing risk and ensuring robust service provision. Furthermore, although they are not directly regulated or supervised by financial services regulators, intragroup service providers are often closely involved in regulatory implementation in the group and dialogue between a group trading entity and their regulator. Intragroup service providers are also contractually bound to help the other entities within the group comply with resilience requirements and therefore are indirectly captured by existing rules. The EU's Digital Operational Resilience Act (DORA) explicitly exempts them from designation as Critical ICT Providers. FIA also notes the FCA Discussion Paper (DP) 22/3 suggests that group service companies would not be recommended for designation (para 4.44 of the DP). If the UK CTP regime deviated from this approach, it could place UK financial services group companies at a disadvantage compared to their peers in the EU.

Question 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?

FIA supports the proposals set out in section 3.12 of the draft Supervisory Statement (SS) that there is no requirement for a CTP whose head office is outside the UK to establish a UK subsidiary where one does not already exist and that the proposals for CTPs are location agnostic.

Regarding designation, FIA members support the approach proposed in section 2.22 of the Consultation Paper (CP) whereby firms and FMIs that are already subject to regulation and supervision/oversight would be unlikely to be recommended for designation as a CTP by HMT.

Interoperability of oversight with other regimes

FIA members support the intent to design the UK's oversight regime for CTPs to be interoperable with that of other regimes, including DORA and the Bank Service Company Act in the US, as set out in 3.15 of the SS.

Furthermore, FIA members support the intent for UK regulators to take into consideration information CTPs provide to other regimes, including DORA and the Bank Service Company Act in the US, in their oversight also set out in 3.15.

Question 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 terms used in them, e.g. 'prudent', 'responsibly'?

No FIA comments on this question.

Question 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?

No FIA comments on this question.

Question 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?

FIA supports the UK Authorities recognizing the importance of CTPs mapping their resources, including the assets, and technology, used to deliver, support, and maintain each material service it provides and expect all elements in the mapping (resources) to be subject to the CTP Operational Risk and Resilience Requirements. However, FIA notes that

it is not expressly clear that the resources included in the mapping would be subject to the CTP Operational Risk and Resilience Requirements. Additionally, FIA notes the mapping should be focused on the resources that are material to the delivery of the material service provided to firms/FMIs; these could come both from assets and technology directly supporting the material service, and from those other internal services which, even if not directly connected to the material services, are nonetheless significant to the functioning of the firm and therefore its ability to provide the material service. A failure in one of the CTP's mapped resources could have a significant impact on their ability to deliver a material service. As a result, we recommend modifying section 5.2 of the SS to say, *"As noted in section 3, the CTP Operational Risk and Resilience Requirements only apply to a CTP's material services, including the resources, the assets, and technology, material to the delivery, support and maintenance of each material service it provides."* This suggested modification will explicitly require CTPs to consider resilience of their resources against the operational resilience requirements.

Requirement 3 (Dependency and supply chain risk management)

FIA members support the approach taken whereby it is the CTP's responsibility to identify and manage risks to its supply chain that could affect its ability to deliver a material service including dependencies on key nth party service providers.

Requirement 6 (Mapping)

FIA members support the requirement for a CTP to identify and document *"any internal and external interconnections and interdependencies between the resources identified in respect of that service"*. While this requirement will require some work on the part of the CTP, FIA members believe it to be helpful. Moreover, as mentioned above, it is important to ensure that CTPs consider the resilience of all material supporting resources as a core objective of the operational resilience requirements. The mapping requirements in 5.31 of the draft SS would require vulnerabilities associated with material support services to be understood, and could, at some point, result in scenario testing of those services. Nonetheless, the overall strategies, controls, processes and systems to ensure the resilience of those material support services would not be applied. FIA suggests that the authorities consider the drafting of the supervisory statement in this regard.

Question 6: Are there any aspects of specific requirements that the regulators should clarify, elaborate on, or reconsider?

Requirement 4 (Technology and Cyber Resilience)

FIA recommends UK Authorities to include the word 'materially' supports a material service in 5.23 to assist critical third parties with interpreting this concept. To provide further clarity, UK Authorities could consider providing a non-exhaustive list of relationships that CTPs should take into consideration recognizing that as a practical and legal matter

each CTP remains obligated to identify and manage its own specific universe of technology assets and subcontracting relationships.

Requirement 7 (Incident Management)

Regarding the proposal that a CTP's response and recovery measures should cover the lifecycle of an incident, including but not limited to *"Procedures and targets for restoring material services and recovering data (e.g., recovery time objectives (RTOs). To the extent possible, these targets should be compatible with the impact tolerances that firms and FMIs have set for important business services.":*

While CTPs may attempt to set the impact tolerances for their material services in line with firms and FMIs, there is evidence that the values set by these institutions varies widely as these institutions continue to work with the UK Authorities to decrease the variance in these values. As noted in speech provided by Duncan Mackinnon, Executive Director for Supervisory Risk Specialists at the City & Financial 9th Annual Operational Resilience for Financial Institutions Summit[1]. Impact tolerances for CHAPS payments have varied from two days to two weeks. Given these observations, FIA recommends the UK Authorities to use firm and FMI impact tolerance measures with caution until such time that financial institutions reasonably decrease this variance so that CTPs have a clearer understanding of the tolerances that their material services should adhere to.

Maximum Tolerable Level of Disruption: We welcome the CPs intention to require CTPs to set a maximum tolerable level of disruption (MTLD). However, FIA recommends additional clarity is provided as to how the CTP would take into account the impact tolerances (ITols) of firms and FMIs. We would therefore recommend that the proposed Requirement 7 (section 5.40 of the draft SS) on Incident Management, Response and Recovery measures is reframed so that the onus is on CTPs to share information about their maximum tolerable level of disruption with firms and FMIs for review to ensure that, over time, their targets become compatible to the extent possible with the impact tolerances set by firms/FMIs for their own important business services, while recognizing that such impact tolerances can vary across the sector.

Question 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?

No FIA comments on this question.

Question 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?

[1] https://www.bankofengland.co.uk/speech/2022/may/duncan-mackinnon-speech-at-the-city-and-financial-9th-annual-operational-resilience

Final incident notification.

FIA requests that the text provides clarity that a notification will be provided by the CTP to the relevant regulatory authority and the firms/FMIs once the incident has been resolved. This notification will allow these affected parties to take appropriate actions to restore their own internal services. Separately, root causes and lessons learned should be provided to the regulators and to firms/ FMIs impacted by the incident at an appropriate timeframe after this notification.

Question 9: Do you have any comments on the regulators' definition of 'relevant incident'?

No FIA comments on this question.

Question 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?

FIA supports the requirements for the CTP to share incident notifications with firms. However, the current definition of incident may be overly broad and result in excessive notifications to firms. We recommend that the definition in 7.4 of the draft SS be changed as follows:

"The incident notification requirements apply to a 'relevant incident', which is defined as a relevant incident ***which*** *is either a single event or a series of linked events that actually or* ***is highly likely to****..."* ~~*has the potential to*~~

Moreover, FIA highlights that supervisory Requests for Information (RFIs) can elicit an extensive effort from the recipient firm and create follow-up activity between the three lines of defence. Therefore, we ask the authorities to consider how they make use of CTP incident reports. Firms/FMIs will use CTP material services in different ways and will have in-place existing risk management, controls, and resilience capabilities for their services such that an incident at a CTP does not necessarily mean a significant disruption to the firms/FMIs' important business services. We therefore recommend authorities exercise discretion when making use of RFIs to avoid generating significant additional work for incident response teams and so as not to overly sway the firm's internal risk assessment.

Question 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?

FIA cautions that some of the requirements in section 7.18 of the draft SS may create additional security risk. The use of the term vulnerability is unclear in this context, specially whether it refers to a cybersecurity vulnerability or a vulnerability in line with how the term is used in the UK's operational resilience supervision. If the term vulnerability in this context refers to a cybersecurity vulnerability, FIA emphasizes that vulnerabilities should not be disclosed before suitable patches are determined and circulated using established channels. Requiring disclosure before that time creates additional risk of widespread exploitation of the vulnerability. We would therefore welcome clarification that the authorities intend this to mean vulnerabilities for the purposes of operational resilience.

Question 12: What are your views on having a standardised incident notification template?

No FIA comments on this question.

Question 13: Do you have any comments on the regulators' proposed rules and expectations in relation to information gathering and testing?

FIA highlights it may be more suitable to think of table-top exercise formats instead of fully fledged testing exercises to comply with the regulators' proposed rules and expectations in relation to testing. The main objective is to renew understanding and validate existing assumptions about how the CTP will respond in the event of an outage. Among other things, the objectives of such sessions could be to renew points of contacts for crisis management between the CTP and firms, to review structures and methods for communications with the markets and to confirm assumptions about response capabilities. Taking an approach less focused on "testing" should allow for more frequent reviews of the playbook and for inclusion of a larger number of firms.

FIA welcomes the requirements for the CTP to test its playbook annually and for firms/FMIs to be included in that testing. FIA members support CTPs having the ability to determine how an appropriately representative sample is determined and to have this method reviewed and agreed to by the UK Authorities given the varying CTPs and associated services that may be in scope and the need to ensure systemically important firms are considered. Similarly, requirements for testing methodology, whether testing the incident management playbook, table-top testing or other

testing methods, should remain outcomes-focused and avoid overly prescriptive or granular requirements that may be challenging to meet for each unique CTP.

FIA believes 6.17 should be expanded to ensure resources, including the assets, and technology, used to deliver, support, and maintain each material service CTPs provide can be included in the possible scope of testing as these will be critical to the functioning of the CTP's material services (see response to Question 5). This could be predicated on the mapping the CTP will have undertaken concerning their material services. F The description of scenario testing in 6.9 should additionally include reference to the assets, and technology, used to deliver, support, and maintain a material service.

Concerning the sharing of assurance and testing information with firms and FMIs (6.23), FIA is concerned that CTPs are required to share information such as the results of scenario testing and financial sector incident management playbook testing, including any recommended remediation, and a summary of the information contained in the CTP's annual self-assessment submitted to the regulators. Sharing confidential or proprietary information with other FMIs could pose multiple risks in terms of disclosing vulnerabilities, individual data, proprietary information, etc. Disclosing vulnerabilities can trigger other vulnerabilities, undermining the spirit of the proposal. The rationale and benefits of sharing broadly a document (i.e. self-assessment information) more relevant for regulators than for other firms are unclear. Therefore, we would suggest following a more proportionate approach ensuring more balance between the disclosing requirements and the effective benefits.

Question 14: What are your views on whether the regulators should include additional mandatory forms of regular testing for CTPs?

No FIA comments on this question.

Question 15: Do you have any comments on the regulators' proposals to require CTPs to share certain information with firms and FMIs?

Related to the draft SS requirement in 7.15, FIA recommends for regulators to consider that CTPs will not know the full impact of the outage on firms and to limit the information asked from CTPs in the immediate follow-up to an outage, as this would increase CTPs reporting requirement to the regulators without more comprehensive availability of information. Since the CTP will not be able to assess the use of its services by firms, or firms' resilience or continuity plans, we expect the CTP will often resort to providing a list of known Financial Services customers. We recognise authorities may wish to make use of this information, therefore we recommend that clear guidelines be developed internally, and a high threshold be applied before RFIs are circulated to firms.

FIA believes there should be no expectation that the sector playbook or industry-wide engagement substitutes for bilateral interaction between the CTP and its impacted customers. Section 5.46 of the draft SS could expand on this

point. As part of crisis management, FIA welcomes the expectation for CTPs to engage with exiting crisis management groups, but we note that the relationship (contractually, business and resilience impact) between the CTP and different firms and FMIs will be different and sector-level information exchange is unlikely to be sufficient for a firm or FMI that is critically impacted.

Question 16: Would the information the regulators propose to require CTPs to share benefit firms' and FMIs' own operational resilience and third-party risk management?

No FIA comments on this question.

Question 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?

No FIA comments on this question.

Question 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?

Misleading Use Of Designation Status

While the draft SSs 8.2 and 8.4 provide clarity to what the designation means and how it can be used, the designation of a supplier as a CTP will provide firms and FMIs with a greater level of visibility into the CTP's operational resilience capabilities; the level of rigor that the CTP has committed to their Operational Resilience programs based on the regulator's eight (8) requirements, and the opportunity to participate in the exercising of the CTPs operational resilience strategies (re: sector-wide exercises, exercises with a reasonable number of its clients). While this is the desired result, there could be an unintended consequence that the ability of firms and FMIs to engage with a CTP at this more granular level may create an environment where firms and FMIs are more likely to select these firms as they are bound, by rule/law, to increase their engagement. It may follow that while the CTP cannot market this designation nor do the regulators recommend or endorse a particular vendor that the effect of this deeper engagement may shift the favour of CTP vendors over those that do not carry the CTP designation. Therefore, the UK Authorities may need to consider the ability to allow vendors that do not meet the CTP thresholds with the ability to 'opt-in' to this regime in order to level the playing field and allow competition for those vendors looking to compete with CTPs that have acquired a significant market share.

Question 19: Do you anticipate any other unintended consequences from the designation of CTPs? Are any further requirements necessary to avoid these unintended consequences?

No FIA comments on this question.

Question 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?

No FIA comments on this question.