UK Finance response to PRA consultation paper 26/23 I FCA consultation paper 23/30 - Operational resilience: Critical third parties to the UK financial sector

Introduction

UK Finance is the collective voice for the financial services industry. Representing around 300 firms, we act to enhance competitiveness, support customers, and facilitate innovation

The UK financial sector's operational resilience and ability to provide critical services depends heavily on third-party technology providers. As such, UK Finance welcomes the regulators' proposals to establish a comprehensive oversight regime for critical third parties (CTPs) to the sector. This consultation response outlines UK Finance's position on the key elements of the proposed CTP regime.

UK Finance strongly endorses the principles-based, outcomes-focused approach adopted by the regulators. Imposing prescriptive, detailed requirements risks stifling innovation and creating challenges for firms operating across multiple jurisdictions. The proposed fundamental rules for CTPs align well with existing principles for regulated firms and financial market infrastructures (FMIs).

A key focus is the resilience requirements for CTPs' material services that support important business services of firms and FMIs. UK Finance broadly supports measures like scenario testing, impact tolerance setting, and demonstrating service substitutability to enhance resilience. However, clarity is needed on aspects such as defining maximum tolerable disruption levels vis-a-vis firms' impact tolerances.

The response highlights the importance of effective incident reporting by CTPs to both regulators and firms/FMIs. Aligning with emerging global standards like the Financial Stability Board (FSB's) FIRE proposals can streamline processes. Calibrating notification thresholds appropriately to avoid alert fatigue is crucial. Thorough testing of CTPs' resilience measures and playbooks, with firm/FMI involvement, is welcomed. However, aspects like selecting the representative firm sample and expanding testing scope to cover internal essential services need further consideration.

Ensuring transparency through information sharing by CTPs on risks, testing results, and third-party dependencies can significantly aid firms' risk management. Appropriate confidentiality safeguards are necessary. The response flags potential unintended consequences like dampening innovation and service provision if regulation is perceived as overly burdensome. Monitoring supplier behaviour and maintaining an adaptable approach is recommended.

UK Finance seeks clarity on implementation timelines, flagging that the proposed three-month self-assessment period may be impractical for some CTPs.

Overall, this response aims to constructively feed into the development of a robust CTP regime that enhances the UK financial sector's operational resilience while avoiding excessive burden or stifling innovation.

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?

For the benefit of both service users and service providers, UK Finance request that all terminology is clarified with an appropriate glossary of terms or a separate definitions chapter at the beginning of the eventual final supervisory statement. To allow for both users and providers of designated services to accurately and efficiently map services, relate dependencies and identify linkages, UK Finance requests that definitions should not deviate significantly from those already set out in related official documents, specifically:

- *Financial Services and Markets Act 2023*
- PRA - SS2/21
- PRA - SS1/21
- FCA PS21/3
- EBA - Guideline on outsourcing arrangements.
- FSB - Enhancing Third-Party Risk Management and Oversight – Toolkit
- FSB – Cyber Lexicon

We request further clarity on the definition of "employee" currently given in chapter 2 (page 4) of the draft supervisory statement (SS) as it could be construed as including a CTP's subcontractors in the supply chain, due to the wording '*whose services, under an arrangement between that CTP and a third-party, are placed at the disposal and under the control of the CTP*. If this is not the intent of the draft SS, we propose that it is made clear that subcontractors do not fall within the definition of "employee".

The definition of 'material services" should include reference to Financial Institution's (FIs') Important Business Services (IBS) as a consideration for identifying CTP material services. It has been recognised from a wide range of stakeholders that the identification of a material service is relative to the service recipient in accordance with their important business service dependencies, i.e., CTPs should not be responsible for identifying and mapping these in isolation.

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?

UK Finance strongly support a proportionate approach that avoids duplication of existing regulatory requirements.

The proposed principles-based approach to regulating CTP to the financial sector is broadly supported by UK Finance's membership. We also strongly endorse the regulator's approach in avoiding additional requirements for firms and Financial Market Infrastructures (FMIs), and instead focusing the regime on the requirements for CTPs.

Providing a more detailed set of requirements may help certain companies better understand and meet regulatory obligations. However, adopting a strict, detailed approach could lead to challenges for businesses in securing positive results, especially given the rapid rate of technological advancements. Negative aspects of a prescriptive approach may be felt most acutely amongst firms and FMIs seeking to apply a unified approach to third-party risk management across multiple regulatory jurisdictions. UK Finance supports the principles based, outcomes focused approach put forth by the regulators for CTP regulation.

The consultation paper indicates that the regulator will rely on a range of data sources to support the identification of CTPs, and that they will consult later in the year on a review of the outsourcing and third-party reporting requirements noting that they may rely on ad-hoc data requests to firms and FMIs in the interim. UK Finance encourages regulators to leverage existing sources of information to the greatest extent possible, and not increase the reporting burden on firms and FMIs by conducting additional ad-hoc data collections in advance of final publication thus pre-empting that consultation in an effort to accelerate the identification process.

Fundamental Rules

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'?.

UK Finance look positively on this proposal and its current scope i.e. limited to the services provided by a CTP to firms and FMIs. The fundamental rules set out in this consultation map closely to those set out in the FCA Handbook (PRIN 2.1 "The Principals) and the PRA Fundamental Rules, for already regulated firms and FMIs. UK Finance would query any significant divergence from these due to a misalignment between the expectations set against regulated financial services (FS) firms and the CTPs.

In addition to the proposed rules, UK Finance recommends the introduction an additional CTP fundamental rule which will require CTPs to co-operate with their FS customers (firms and FMIs) as they seek to meet their own regulatory obligations[1].

By concentrating oversight efforts on material services, regulators can effectively address systemic risks without imposing undue burden on non-material functions. This is consistent with the principle of proportionality, ensuring that regulatory requirements are commensurate with the impact of services provided.

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?

UK Finance agree that it is sensible and correct for the Fundamental Rules to apply to all services provided by CTPs to financial firms and FMIs.

Operational Risk and Resilience Requirements

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?

UK Finance broadly welcome requirements for a designated CTP to demonstrate substitutability of services provided to the financial sector. This process would not only assist financial firms and FMIs to establish operationally viable exit plans for those material services that support their important business services and thus increase operational resilience, but would alleviate concerns over "vendor lock-in" and promote a competitive environment for the provision of certain services that could ultimately reduce vulnerabilities caused by systemic concentration risk.

By focusing on material services, regulators can enhance the sector's overall resilience without stifling technological advancements. We emphasize the need for flexibility in implementation, recognizing that CTPs operate in diverse contexts and serve varying functions.

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

[1] This would include an obligation to engage with customers on matters of due diligence, attestation etc.

There is some concern that the current proposals set out in paragraph 5.5 of the draft supervisory statement could lead to CTPs appointing an insufficiently senior individual to oversee the CTPs' compliance with the regime. We would encourage the regulators to set out more clearly their expectations for the seniority of the designated individual(s), to ensure consistency amongst CTPs.

UK Finance would support harmonisation of key concepts between the operational resilience requirements for CTPs and those for banks. As such, we would propose changing the terminology from "a maximum tolerable level of disruption" to an "impact tolerance".

We welcome the CPs intention to require CTPs to articulate a maximum tolerable level of disruption (MTLD). However, we are unsure how the CTP would take into account the impact tolerances (ITols) of firms and FMIs. We suggest alternatively that CTPs should be required to document their MTLD and share this information with firms and FMIs who utilise the respective service. This should also be required for the CTPs "internal essential services". Firms and FMIs can then use this information to plan their own resilience, or negotiate with the CTP to improve their MTLD.

Regarding Incident management, it would be helpful for the regulators to extend the proposed requirements for CTPs to implement measures to respond and recover from incidents, to also implement measures to identify, protect and detect incidents, in line with other widely adopted industry standards.

UK Finance welcome complementary regulation. As such, we are keen to gain assurances that the resilience requirements set out in existing regulation (SS2/21 specifically) are thoroughly deconflicted with the CTP regulation so as not to create undue burden or clashes.

Section 5.42 and 5.43 of the CP proposes to require a CTP to have in place appropriate measures to respond to a termination of any of its material services. The draft supervisory statement sets out a non-exhaustive range of reasons why termination may happen, including but not limited to corporate restructuring, change in control, legal or regulatory issues, insolvency, court processes, or unrecoverable disruption. Firms and FMIs would remain responsible for complying with applicable requirements and expectations on operational resilience and third-party risk management, including in relation to stressed exits. We welcome the requirements for the CTP to have in place appropriate measures to support the effective, orderly and timely termination of services including (if applicable) their transfer to another person, including the firms or FMIs the services are provided to. However, UK Finance would welcome further clarity on the regulatory expectations on a CTP regarding the type of assistance that they should provide firms to effect their own exits from the CTP in the event of a termination of contract.

CTP material services may, on occasion, require transfer to another provider. In order to gain an equivalent level of service, a firm or FMI may face substitutability or interoperability difficulties. UK Finance propose that the termination requirements set out in Requirement 8 to be applied to any other CTP should they be the party that the material service is being transferred to. We recommend that any CTP should take all reasonable steps to ensure the participation and collaboration of another CTP, or provider, in the transfer of material services to that CTP or provider. In addition, a CTP should take all reasonable steps to not disrupt or discourage any termination or transfer of material services to another provider, such as through deliberate commercial or technology impediments.

Further on incident management, response and recovery measures in relation to CTP procedures and targets for restoring material services and recovering data, says: "To the extent possible, these targets should be compatible with the impact tolerances that firms and FMIs have set for any important business services, which are in turn supported by the CTP's relevant material services."

This indicates that firms and FMIs will need to disclose to CTPs which services support which IBSs, as well as the impact tolerances for those IBSs. Members would not be supportive of sharing this information, due to both the uplift of data and reporting burden, and concerns around confidentiality. As an alternative, when designating a CTP, the authorities could give anonymised information on the most relevant (e.g. lowest) impact tolerance for designated material services based on information collected from firms and FMIs under existing frameworks.

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?

Given that some of the hyperscalers (likely to be designated as CTPs under this regulation) offer "*over 200*" distinct services[2], UK Finance strongly support the proposal for a limitation of the scope of operational risk and resilience requirements to apply to a CTP's material services only.

Any extension or broadening of this scope will almost certainly result in additional resource expenditure to the CTP without any tangible benefit to effective risk management and enhancing the operational resilience of the financial sector.

The CP explicitly applies to the material services of the CTP. We welcome the focus on what is material to the dependence the financial sector has on the CTP. However, we believe clarification is needed about how far this requirement goes. In particular, there will exist services, technology, or third-party providers (TPPs) that are material to the CTP overall and not specific to a service identified as material for the purposes of the UK regime. These services will likely be listed by the CTP under the assets and technology that support material services within the mapping requirements. A failure in one of these services, systems or TPPs could have significant impact on the services identified as material. Such services could be called internal essential services. We believe that these services should also be in scope for all operational risk and resilience requirements in section 5 as their failure could have systemic impact on the functioning of the financial system. For example, major outages at cloud providers have in the past come from failures to internal services such as domain name system (DNS), Active Directory (AD), security certificates or identity and access management (IAM) which, in turn, prevented the use of external services by clients. Ensuring that CTPs consider the resilience of these "internal essential services" should be a core objective of the operational resilience requirements.

5.2 of the draft SS could be interpreted to narrowly apply to the external service, however, statements within the requirements such as 5.13 to effectively manage risks to its ability to continue to deliver a material service could include consideration of internal essential services. The mapping requirements in 5.31 would require vulnerabilities associated with internal essential services to be understood and could result in scenario testing of those services at some point. Nonetheless, the comprehensive strategies, controls, processes, and systems to ensure the resilience of those internal essential services would not be applied. We suggest that the authorities consider the drafting of the SS in this regard and whether clarity can be provided as to the depth that the requirements reach into the CTP.

Incident Reporting

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?

UK Finance agree that the identification and notification of incidents (defined below under Q.9) is imperative for the effective functioning of any sector reliant on the use of third parties to support their important business services. In addition to striking the right definition of "incident" / "relevant incident", the calibration of the threshold of such incidents is critical to the effective functioning of

[2] https://www.aboutamazon.co.uk/what-we-do/

any system or set of regulatory obligations that demand them to be reported. The level of detail provided must be sufficient for firms to understand the impact on the services in scope.

UK Finance would welcome more granular detail from the regulator on what may or may not be / should or should not be regarded as an incident. While the CP references “cyber-attacks” and “natural disasters” as categories, we would want to promote close alignment among designated CTPs on their respective thresholds in order to ensure clarity for the service user.

We welcome the requirements for the CTP to share incident notifications with firms. However, we note that the current definition of “incident” may be overly broad and result in excessive notifications to firms. We recommend that the definition be changed as follows:

- The incident notification requirements apply to a ‘relevant incident’, which is defined as either a single event or a series of linked events that actually or **is highly likely** to: [*then continue as per the draft ss*]

In addition, we wish to caution the authorities regarding how they make use of CTP incident reports. We recognise that authorities plan to utilise third-party registers to identify firms and FMIs that may be exposed to an incident from a CTP. However, as per our comments above, the actual impact of an incident as a CTP can vary significantly between firms depending on the use of the service, their role in the market and the CTP’s interpretation of the incident reporting scope. Firms, in addition, have existing risk management controls and mitigation policies in place for their services and incidents may not see any internal or external impact to a firm’s service. Supervisory RFIs can elicit an extensive effort from the firm and create follow-up activity between the three lines of defence. They can also influence internal perspectives on the seriousness of an incident, sometimes in contradiction to what the actual operational risk assessment of the firm might be. We therefore recommend authorities exercise discretion when making use of this tool so as to avoid generating significant additional work for incident response teams and so as not to overly sway the firm’s internal risk assessment.

Connected to this issue, 7.15 of the draft SS requires the CTP to provide the authorities with information regarding the firms and FMIs impacted and details on the nature of that impact. We believe that it will be exceedingly difficult for CTPs to identify this information, especially for the initial report. Given 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 FS customers. If supervisors act on this information it is likely to lead to a significant amount of additional work for incident responders within FIs, in line with our comments above. While we recognise authorities may wish to make use of this information, we recommend that clear guidelines be developed internally and a high threshold be applied before RFIs are circulated to firms. This is particularly true if incident reporting requirements evolve to necessitate a substantially greater amount of information from firms, thereby intensifying the operational impacts of such reporting on firms.

We have some reservations about certain requirements within section 7.18 of the draft SS, as they may potentially introduce additional security risks. The use of the term vulnerability is unclear in this context, specially whether it refers to a “cybersecurity vulnerability” or a “vulnerability” as the term is used in the UK’s operational resilience policy. If the former, the industry believes 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. It is also the case that certain jurisdictions may attempt to require such information be reported for the purposes of building their own databases of vulnerabilities. We would welcome clarification that the authorities intend this to mean vulnerabilities for the purposes of operational resilience.

While we welcome the expectation that CTPs engage with existing sector crisis management groups, we believe it is important to be clear that this does not replace the expectation that they engage directly with their customers during an incident. 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. By way of example, in the ION incident there was wide discrepancy between different firms who were clients of ION, with some experiencing material disruption while for others there was limited impact. There should be no expectation that the sector playbook or industry-wide engagement substitutes for the bi-lateral interaction between the CTP and its impacted customer. Section 5.46 in the draft SS could expand on this point.

Finally, we recommend a phased approach to incident notifications, allowing CTPs to escalate appropriately based on severity. The framework should strike a balance between responsiveness and practicality.

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

The CP (7.6) sets out the definition of "relevant incident" as:

"…either a single event or a series of linked events that actually or has the potential to:

- *seriously disrupt the delivery of a material service; or*
- *seriously and adversely impact the availability, authenticity, integrity or confidentiality of assets relating or belonging to the firms which the CTP has access to as a result of it providing services to firms or the potential to result in a serious loss of such assets."*

In addition to the previously mentioned revision of this definition, UK Finance would welcome further clarity on the definition of "seriously" and what thresholds would be used to determine what it constitutes..

Under paragraph 7.6 of the draft SS, the regulators note that when assessing whether an incident meets the definition of a relevant incident, CTPs should consider their internal management of the incident. For clarity, this could be enhanced to specifically state that any incidents or events which were classified as high severity by the CTPs, including those with a material impact on or risk to FMIs, firms or material outsourcers.

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?

Some concern has been expressed about the possibility of "alert fatigue" within service recipients in the event that the threshold for a "relevant incident" (as set out in chapter 7 of the Draft SS) is set too low resulting in a high volume of reports. As previously stated, we would strongly recommend that consideration is given to linking what is judged to be a "relevant incident" to breaches of impact tolerances.

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?

UK Finance is working with the Financial Stability Board on the "Format for Incident Reporting Exchange (FIRE)" concept (LINK), itself a product of the FSB's Recommendations to Achieve Greater Convergence in Cyber Incident Reporting (LINK).

To reduce the burden on all stakeholders within the financial services sector we encourage any incident reporting proposal to harmonise with existing formats. We recognise that the creation of multiple similar (yet different) formats and types of information required to fulfil them ultimately slows incident response times due to resources being allocated towards the generation of avoidable bureaucracy and not incident resolution.

Furthermore, it would be helpful for the initial and intermediate notifications to additionally include information regarding:

- Reliance on other third parties;
- Known downstream impacts; and
- Recommended actions to be taken by customers.

The final Notification should include information pertaining to:

- Details of any post mortem reviews / assessments to be carried out
- Client communications
- Any additional monitoring required

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

While templates can be important to enable the effective ingestion of structured information into the service user’s environment, they may also promote a rigidity that obscures the true nature of an incident from the service user. Due to the diversity of incidents that may fall within the “relevant incident” category, a singular template may be problematic. UK Finance recommend harmonisation with the proposals set out in the FIRE proposals , and ensure that sufficient flexibility is embedded to allow CTPs to provide additional, and descriptive information with any incident report.

Testing

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

We welcome the requirement for CTPs to test their playbook annually and for firms to be included in that testing. However, it is unclear how the representative sample in 6.17 is to be chosen. It may be better to think not of testing in the sense of fully fledged exercises, but rather something more akin to a table top exercise, the main objective of which is to renew understanding and validate existing assumptions about how the CTP will respond to an incident. 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.

For the stability of the UK’s financial system, it is critical that a CTP is able to maintain its ability to provide material services to FS customers and clients. UK Finance believe that CTPs should thus take all reasonable steps to ensure the continuity of service provision even when faced with a relevant incident. CTPs should consider underlying technology when setting out to maintain this continuity of service. As such, the regulator could consider an expansion of the provisions set out in 6.27 to include testing carried out on internal essential services as these will be critical to the functioning of the CTP’s material services. This could include reference to the processes or technologies used to deliver, maintain or support a material service and be predicated on the mapping the CTP will have undertaken concerning their material services. In order to emphasise the importance of internal essential services, the regulator could consider the expansion of requirements in 6.13 to include a further bullet on “the assets and technology that deliver, support, and maintain that essential service.” The description of scenario testing in 6.9 should additionally include reference to the internal essential services for the material service.

6.7 of the CP sets out a general requirement that a designated CTP would be required to demonstrate compliance with rules on an annual basis and "upon request". UK Finance would like to know more about the circumstance that may prompt such a request.

UK Finance believes provisions regarding the scheduling and annual cadence of testing (as set out in Appendix 4 chapter 6.12) would likely result in a singular batch of testing being conducted in or around the same time period annually. Given this, we would welcome the consideration of the staggering of this requirement to allow industry participation on the incident playbook testing activities which would not be feasible if they were all to occur at the same time each year.

6.13 of the draft SS sets out that a CTP is responsible for identifying the scenarios it will test, taking into account prior disruption to its services, operations, and supply chain. It may be helpful to include both lessons learned from the CTP's own experiences and peer organisations.

To bring practice in line with common industry practice, it may be helpful to expand on 6.14 of the draft statements where it sets out the minimum considerations for scenario design to include:

- Under supply chain, to include the stressed exit of a key supplier
- To add a fourth bullet point covering climate related events or disruption of energy supply.

Scenario testing should also parallel/support the testing that FIs need to perform. We encourage the regulator to recommend that FIs and CTPs coordinate in testing to avoid any duplicative testing, or redundant testing that is not relevant to the FI.

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

UK Finance supports the proposal for annual testing as set out in the "Testing Requirements" section of appendix 4. In addition to the testing proposed, a requirement for CTPs to conduct regular Continuity of Business testing, covering at a minimum unavailability of technology (denial of service), unavailability of primary work location (denial of access) and unavailability of staff (including subcontractors). The results of this testing should also be provided firms and FMIs on an annual basis.

While UK Finance is aware of the potential for additional requirements on firms, FMI and CTPs to supress the willingness of service providers to serve the financial sector, it is our assessment that the addition of this continuity of business (CoB) testing strikes the right balance.

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

The draft SS (Appendix 4 chapter 6.36-6.37) sets out that a designated CTP must have effective and secure processes and procedures in place to ensure sufficient and timely information is given to the service recipient to enable them to manage risks related to the service.

While UK Finance agrees with this approach and the subsequent requirements that highlight that some confidential or sensitive information may be omitted from reports to firms and FMIs that will however be needed by the regulators, we believe more consideration should be given to what types of information might be considered "confidential or sensitive". Additionally, more definitive timelines may help in ensuring that the regulatory expectation is clear e.g. "within three months" opposed to "sufficient and timely" may be less ambiguous and sets a clear limit on both parties.

To support firms' interpretation of the results of scenario testing, the regulators should also require CTPs to provide information on the scenario which was tested against. Additionally, in line with our comments on question 6, it would be helpful for the results of the testing to be framed around IToLs.

In addition to the information already covered in the proposals, it would be helpful for firms and FMIs to receive additional information from CTPs, including:

- Consolidated information on subcontracting – this would streamline the process of firms and FMIs individually seeking information on subcontracting on a bilateral basis (specifically where not being provided under existing regulatory frameworks).

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. The proposal to require CTPs to inform service users about actions taken in the light of test results could be used to inform a firm's risk management plans and documentation.

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?

UK Finance assesses that the proposals adequately balance confidentiality with the advantages of sharing information.

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? 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?

UK Finance is supportive of the measures aimed at prohibiting the active use of CTP designation as a pseudo-marketing aid. Regardless of restrictions placed on the official and overt use of designation by the CTP themselves as a marker of resilience or regulator endorsement, it is likely that some firms or FMIs will look positively upon the additional testing requirements and mandated information sharing requirements and may make service procurement decisions based on this.

Furthermore, UK Finance accept that the open publication of the standards required of CTPs by the regulator may cause firms that are outside the designation criteria to voluntarily adopt the testing, information sharing and operational resilience measures required and thus increase the general standards of suppliers to the UK's financial sector.

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

Many UK Finance members are concerned about the potential impact that additional regulation may have on the provision of innovative services to the financial sector. There is a risk that placing additional regulation on CTPs may suppress their appetite to serve, supply, develop and innovate technology services provided to financial services customers, choosing instead to focus on less regulated sectors such as media, retail or consumer technology etc.

There are feasible scenarios in which CTPs embrace their central role in financial services and lead a cultural shift across suppliers in promoting resilience and transparency. Equally, there is a risk that some key CTPs could exit the financial services market in the UK which could leave gaps in the market and ultimately reduce the resilience of UK financial services. Alternatively, there could be an ongoing cycle of increased costs due to CTP designation leading firms to move to alternative suppliers, causing CTPs to then drop below the CTP thresholds. Given the complex and dynamic nature of possible knock-on effects of the CTP regime, the regulators will need to closely monitor changes to supplier behaviour, and approach the framework with a degree of flexibility.

20. Do you have any comments on the cost-benefit analysis?

UK Finance understand the requirement for the cost benefit analysis and, upon review, find no significant issues with the methodology used in the collation of cost estimates. UK Finance agrees with the assessed benefits of the implementation of the CTP regime including improvements to UK financial stability and market confidence, benefits to behaviour and innovation in the market, and benefits to consumers of financial services.

Additional Issues / Questions to the Regulator

1. **Implementation Timelines**: Engagement with various industry stakeholders has highlighted the ambitious (but potentially unachievable) timelines for some CTPs to conform to under the current proposals. The 3-month period for self assessment (once designated) is widely cited as potentially problematic and an extension to this period is requested for consideration. UK Finance members strongly support measures and timelines that will enable designated CTPs to achieve their obligations with accuracy and thoroughness. In addition to the extension to the 3 months self assessment window, UK Finance requests CTPs are afforded a 12-month implementation period for these new regulations. UK Finance also request further communication from the regulators on when they foresee this regulation will be in place by.

2. **Explicit exclusion of certain entities**: UK Finance members believe that this regulation should explicitly exclude institutions (such as third country FMIs) from being designated as a CTP. This is especially so where these institutions are already adequately supervised by competent overseas authorities, and where appropriate cooperation arrangements exist between these home authorities and the UK authorities. Whilst we are aware that section 2.23 of the CP states that "*The regulators are also unlikely to recommend certain third parties in other sectors (e.g. public telecommunications providers, energy suppliers) for designation if the regulators are satisfied that the services that that these third parties provide to firms and FMIs are subject to a level of regulation and oversight that delivers at least equivalent outcomes to the proposed regime*", we would welcome third country FMIs being explicitly in the list of examples of entities provided that are unlikely to be recommended for designation.

Additionally, UK Finance believes that intra-group services companies should also 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 effectively managing risk and ensuring robust service provision. Further, 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 DORA already recognizes the reduced risk associated with intragroup providers and explicitly exempts them from designation as Critical ICT Providers. If the UK CTP regime deviated from this approach it could place UK financial services group companies at a disadvantage to their peers in Europe.

3. **Data Collection**: We note that section 2.6 of the CP states that "Over the past few years, the regulators have undertaken ad-hoc data collections relating to firms' and FMIs' OATP arrangements. Data collected in this way will continue to inform the regulators' recommendations for designation until the proposed OATP register is operational." We hold the view that it's essential for the regulators to apply their authority judiciously and with an awareness of the potential risk that the suggested powers for information collection and auditing might place undue strain on FMIs that

are already under the effective supervision of objectively proficient central banks and securities regulators abroad.

4. **Self Assessment**: Section 6.2 - 6.8 of the draft SS covers the requirement on CTPs in regards to self assessments. UK Finance requests that regulators require CTPs to provide their annual self-assessment in full (redacted where appropriate) instead of a summary so that there is a consistent application by CTPs of this requirement.

If you have any questions on this response, please reach out to:

UK Finance:
Adam Avards, Principal, Cyber and Third Party Risk
adam.avards@ukfinance.org.uk