Consultation Response

CP26/23: operational resilience: *critical third parties to the UK financial sector*

March 2024

AFME welcomes the opportunity to respond to the consultation paper by the Bank of England (BoE)/ Prudential Regulation Authority (PRA) on ***Critical Third Parties to the UK financial sector***[1] **(CP 26/23)**.

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors, and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

We are responding from the perspective of our bank members and have focused on those issues which are most relevant to wholesale capital markets. Given the level of interest in this consultation we have responded to each of the questions within CP 26/23 and we remain available to discuss any of the specific answers in further detail. We also look forward to engaging on both data collection and enforcement powers in due course, as part of these upcoming reviews.

In addition to our responses below on each of the posed questions, we raise these three broader points:

1. **Scope of UK regime:** The consultation paper states that it is "unlikely" entities which are already regulated will be designated under the UK regime. Clarification is required, particularly whether this relates to regulation by financial services authorities, either UK or international, or instead to entities regulated by non-financial authorities, for example communications or data regulators. We would welcome explicit confirmation that intragroup providers are not within scope and stress that with DORA's (the EU Digital Operational Resilience Act's) more explicit parameters, the market is largely working on the assumption that digital providers, especially CSPs (cloud service providers), are the likely targets for future designation. Attempts to broaden this regime to capture entities who are not technology providers, for example wholesale cash distribution providers, will cause concern and should be adopted through clear and early signposting with industry. We also note that the BoE intends to consult separately on enforcement, and agree this issue requires further engagement, especially given the difficulties of enforcement which flow from most providers remaining outside the CTP regulatory perimeter.

2. **Data Collection & Input:** Noting that the BoE intends to consult separately later in the year on data collection, we have largely reserved our feedback on data input requests. We do though stress that information on the Important Business Services (IBS) of financial institutions (FIs) is already available to authorities and should be lifted from existing databases/reporting. If further data requests are required, for example due to the lack of legal powers over CTPs prior to designation, we urge the BoE to exercise

[1] Bank of England, CP26/23 – Operational resilience: Critical third parties to the UK financial sector, 7 December 2023, CP26/23 - Operational resilience: Critical third parties to the UK financial sector | Bank of England

restraint until the subsequent consultation is concluded, especially in relation to Nth party providers where there is a widely recognised issue in terms of availability of data from an FI's perspective. In future, we also note that CTPs will be better placed to provide in-depth transparency over the supply chain.

3. **Contract remediation:** While not explicitly called for within the consultation paper, we envisage that designated CTPs may have to update or amend their contractual arrangements with clients. Any contractual uplift comes with a significant burden for FIs, given the hundreds of arrangements which an FI may have with one CTP and the fact many of these services may be bundled within global framework agreements. Any supervisory expectation for CTP requirements to be reflected in contractual arrangements should be phased in, and permitted as contracts come up for renewal, rather than off-cycle.

Consultation Questions

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?**

   The proposed terms and concepts are generally clear and well understood. AFME would though make two points:

   i. **Material Services:** AFME welcomes the decision not to simply classify all services which support a FI's IBS as *material*. As set out in our response to the DP 3/22[2], not all services deemed material or critical at the individual firm level, will be material at the systemic level. We would though welcome an explicit reference to FI's IBS as part of the definition, given the importance of ensuring the CTP regime cascades from the financial services sector. We would also encourage the authorities to reflect the systemic nature of these services in the actual terminology. We recommend:

Existing wording	Proposed wording
Material service is a service (wherever carried out) provided by a CTP to one or more firms a failure in, or disruption to, the provision of which (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system	**A systemic** ~~Material~~ service is a service (wherever carried out) provided by a CTP ***which supports a firm's Important Business Services and where*** ~~to one or more firms~~ a failure in, or disruption to, the provision of which (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system

[2] AFME, consultation response, DP 3/22: operational resilience: critical third parties to the UK financial sector; https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20Final%20Response%20to%20BoE%20FCA%20PRA%20Critical%20Third%20Parties%20DP.pdf

We additionally note that CTPs should be listing those assets and technologies which support material services within their mapping requirements. A failure in one of these underlying services or systems, or related providers, could have significant impact on the delivery of material services. 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 resulting systemic impact. For example, major outages at CSPs have in the past come from failures to internal services such as DNS, AD, security certificates or identity and access management 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. It would ensure consideration of the broader operational capability of CTPs, including the operationalisation of recovery capabilities. We note that section 5.13 of the draft supervisory statement (SS) would require CTPs to effectively manage risks to its ability to continue to deliver a material service. This could in theory capture consideration of *internal essential services*. Nonetheless, we suggest that the authorities explicitly set this out within the drafting of the SS in this regard.

ii. **FSB Cyber Lexicon:** We welcome the incorporation of the FSB terminologies, and references to the Cyber Lexicon. The harmonisation of terminologies and concepts is one of the most effective ways in which to embed the global attempts at convergence. We suggest at Q9 how this could be further bolstered by the BoE.

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?

AFME members have welcomed the adjustments in the latest consultation document aimed at dialling down the level of burden facing FIs and locking in alignment with the existing operational resilience framework. While the consultation paper states that the CTP regime will not reduce the regulatory obligations facing firms, we have always been of the view that firms will see their burden of responsibility increase as part of the establishment and maintenance of this incoming framework. This especially seems the case on incident management, where we understand FIs will not only be required to enact remedial actions in light of notifications from CTPs, but to liaise with authorities on such measures. We look forward to engaging with the BoE on the upcoming data collection consultation, where we remain confident that most of the information required for designation purposes is already available to authorities. We stress again there should be no expectation on firms to act as agents of the authorities in future supervision of the incoming regime.

The proposal to distinguish between a CTP's material services, versus all services, raises again the need for the BoE to ensure that those services defined as material are linking to a FIs IBS, albeit it with the further requirement that any related disruption could truly threaten systemic stability. It is our recommendation that the authorities, rather than the providers themselves, should designate which of a CTP's services are material, based on the information available to them from FIs and in due course CTPs themselves, or via the representations which can be made by providers who have been notified they are at risk of designation. To alternatively request the CTPs to designate which of their own services are material raises a set of challenges in terms of their limited visibility, especially how they would get sight of an FI's impact tolerance levels. Aggregated data would appear to us too limited to provide meaningfully direction.

The distinction of services must also not lead to broader risks to the provider as an entity being overlooked, for example the risks of material financial stress which could impact the entirety of a CTP, and consequential disruption of CTP's material services.

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, eg 'prudent', 'responsibly'?**

   AFME has no objections or further comments on the proposed Fundamental Rules.

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?**

   In light of the high-level nature of the proposed Fundamental Rules, AFME has no objections to their application to all of a CTP's services.

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?**

   In principle, AFME supports the extension of these operational risk and resilience requirements to CTPs. To date, varied attempts to supervise such entities indirectly through FIs have raised a plethora of challenges, given the inappropriateness of such tasks sitting with the private sector. The enhanced robustness of financial services' supply chains is recognised as a win for the sector and will help ensure that FIs and tech providers are on a level playing field in coming years.

   We specifically call out the following:

   i. **Dependency and Supply Chain Risk Management:** transparency over subcontractors, and any nth Party Providers, has long proved a pain point for FIs, especially in terms of how such entities are compelled to provide certain information. It is likely these challenges will persist with regards to providers outside the CTP regime.

   ii. **Termination of Services:** We welcome the specific obligations on ensuring that CTPs must put in place arrangements to support the effective, orderly, and timely termination of services. In the case of CTP material services, we stress though that alternative solutions may not be available, and that termination should be regarded as a matter of last resort. We suggest below at Q19 this could include consideration of substitutability.

   iii. **Maximum Tolerable Level of Disruption:** We welcome the authorities' 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, as proposed in the consultation paper as part of the measures on Incident Management, Response and Recovery. ("*To the extent possible, these targets (MTLD) 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.*"). 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. Firms and FMIs can then use this information to plan their own resilience or negotiate with the CTP to improve their MTLD. Members would not be supportive of providing information on their IBS with CTPs, due to both the uplift in reporting burden, and concerns around confidentiality. Consideration should also be given to how the prioritisation of recovery will be managed by CTP, its clients, and regulators. In the current guidance the approach is not clear from an accountability or responsibility perspective.

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

AFME members are mindful that for many designated CTPs this may be the first occasion where key individuals within the provider will be subject to this level of regulatory expectations. While FIs are familiar and comfortable with these obligations, it is unlikely that providers will be able to draw on the same level of experience. We encourage open dialogue between CTPs and authorities, to reduce the risk of unintended consequences, by for example providers misjudging the depth of expectation and having to execute remedial measures.

In relation to governance, there is a concern that the current proposals set out in paragraph 5.5 of the draft SS 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.

Additionally, we 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."

Regarding incident management, the draft SS requires CTPs to implement measures to respond and recover from incidents. It would be helpful to extend this to also require the implementation of measures to identify, detect, and protect the CTP from incidents, in line with industry standards such as NIST.

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?**

As per our comments in Q1, we believe that the Operational Risk and Resilience Requirements should also apply to 'internal essential services'.

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?**

AFME strongly supports the proposal for CTPs to separately notify firms of relevant incidents. Policy discussions on a CTP regime are now relatively mature, but there was originally a degree of concern that direct oversight of providers could lead to FIs being by-passed in the immediate aftermath of an incident. We again stress the industry's firm expectation that CTPs engage directly with their customers during an incident. The relationship between the CTP and specific 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 SS could expand on this point.

We additionally stress that while notifications are necessary, follow-up interactions between the FI and provider can be of most value in assisting FIs determine the potential impact on their own services and IBS. It should therefore be anticipated that FIs can respond to notifications to seek follow up information and that providers be obligated to respond within reasonable timeframes and without undue delay. Conversely, we stress that not all notifications from CTPs will require an FI to formally invoke incident response procedures, based on an internal assessment of the potential impact. This should be formally recognised by authorities with regards to their supervision of FIs.

In addition, we wish to caution the authorities on 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 as a supplier. FI/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 FIs/FMIs IBS. Supervisory RFIs (requests for information) can elicit an extensive effort from the recipient 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 the actual operational risk assessment of the firm. We therefore recommend authorities exercise discretion when making use of this tool to avoid generating significant additional work for incident response teams and to not overly sway the firm's internal risk assessment.

Connected to this, section 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 the 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 response teams 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 especially the case if incident reporting requirements evolve to require significantly more information from firms thus exasperating the operational impacts of such reporting on firms.

Finally, we are concerned that some of the requirements with 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 as the term is commonly used in the UK's operational resilience supervision. 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 for the purposes of building their own databases of vulnerabilities. We would therefore welcome clarification that the authorities mean vulnerabilities for the purposes of operational resilience.

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

AFME strongly supports leveraging and supporting the FSB's work on international harmonisation and convergence in incident management and response where possible. We do so in the knowledge that our members regularly use such materials as valuable resources for further guidance. We note though that the definition of "asset" within the FSB Cyber Lexicon is "*Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation*." This omits the inclusion of *data*, which we assume is intended to be within scope of the BoE's proposed definition on "relevant incident." To ensure consistency we propose therefore that the BoE insert an additional sub-element relating to the impact on data, having removed this from scope of asset. We also believe the current definition is overly broad and will result in excessive notifications to firms. We recommend specifically:

Current wording	**Proposed Wording**
"a relevant incident is 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".*	*"a relevant incident is either a single event or a series of linked events that actually or* ***is highly likely*** ~~*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;* ***or*** • ***seriously and adversely impact the availability, authenticity, integrity, or confidentiality of data relating or belonging to the firms which the CTP has access to as a result of it providing services to firm or the potential to result in a serious loss of data."***

Under paragraph 7.6 of the draft SS the authorities 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?

AFME welcomes the alignment with existing practice and using the proposed terminologies for each phase of notification. We stress though that flexibility will often be key, for example with regards to specific data fields under each phase or even whether all three phases are even required.

Our priority is that CTPs should provide updates at regular intervals, and most importantly the notifications need to be timely and regular so that firms can react and apply relevant safeguards, even if there are elements not yet known. Completeness of information should not get in the way of timeliness. Flexibility on the timing of each phase will also assist FIs in meeting various jurisdictional requirements.

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?

AFME recognises that not all information will be available for each stage of notification. We advocate flexibility, with providers able to provide the information across the three phases collectively. Mandating certain information at each stage creates the risk of notifications being delayed or resourcing between deployed at reporting rather than at incident mitigation. The emphasis should be on timely reporting of incidents to customers, rather than on completeness of the reports, and the option to update, add or amend information following a notification should be embedded within the requirements.

The initial and intermediate notifications could be further enhanced by the inclusion of information on:

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

The Final Notification should also include:

- Details of any postmortem reviews / assessments to be carried out;
- Client communications; and
- Any additional monitoring required.

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

Flexibility is the priority for the reporting of information. If a template were to be proposed by authorities, it should include ample descriptive sections to allow for the provision of more qualitative information, especially at the earlier stages of an incident.

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

AFME comments focus on the following rules:

i) Testing: Our primary concern is the risk of duplicative testing on the same underlying services, potentially in parallel, by a CTP and a FI. There is minimum if any value from CTPs and FIs both conducting essentially repeat testing on the resilience of the same service. This appears most at risk of occurrence with regards to the annual testing of the CTP's financial sector incident management playbook. Conversely, the testing of the playbook should be framed in a way that ensures it is also of value to the FI, and that both FIs and CTPs are each able to rely on the test results, with coordination under the mandate of the regulators, and with mutual recognition by authorities providing an important incentive for ensuring participants approach these exercises as a learning opportunity. It is also unclear how the representative sample in 6.17 is to be chosen. We recommend such testing take the form of tabletop exercises, the main objective of which 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.

Guidance is also required on how testing of the playbooks would work in practice, especially given the scale of the coordination challenge with these combined exercises. Guidance should take account of current operational constraints, for example limitations on live production testing, and instead address:

- Accountability and ownership of the exercise, including veto rights by FIs.
- Joint decision-making, including over testing techniques and suitability of testers.
- Remediation plans, and subsequent monitoring of recommendations, especially if authorities envisage potential actions for FIs.

Our recommendation is that authorities formally recognise, potentially on a voluntary basis, existing exercises, rather than looking to establish new tests from scratch. This is especially the case with those forms of testing which are more intensive to apply, for example TLPT and other real-time simulations. The Quantum Dawn cyber simulations which are run by AFME's sister association SIFMA, have recently been extended to enable third party provider participation.

ii) Internal essential services: In addition, we believe 6.27 should be expanded to ensure it also includes testing carried out on *internal essential services* as proposed in Q1 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 which the CTP will have undertaken concerning their material services. In order to emphasise the importance of internal essential services, we believe that the requirements in 6.13 should be further expanded 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.

iii) Information gathering: We support the information gathering provisions within the consultation paper. CTPs will in particular be able to provide regulators with a much greater quality of information relating to subcontractors and Nth party providers. This has typically been an area where FIs have struggled to gain full and enforceable transparency across the entire supply chain. Authorities should in future have first-

hand access through these provisions. To maximise the value of this information, it will though be critical for authorities to ensure FIs have adequate sight of key risks and vulnerabilities. Please see Q15 for further information.

We also flag that 6.13 of the draft SS sets out that a CTP is responsible for identifying the scenarios it will be testing, taking into account prior disruption to its services, operations, and supply chain. It may be helpful to include in this not only lessons learned from the CTP's own experiences, but also those of peers.

In order to bring more in line with industry practice, it may additionally be helpful to expand on 6.14 of the draft SS which sets out the minimum considerations for scenario design, in order to:

i. Include, under supply chain, the stressed exit of a key supplier.

ii. Change "Technology and cyber resilience" to "Its technology and cyber security;" and

iii. Add a fourth bullet point covering climate related events or disruption of energy supply.

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

Testing at present seems to more align to traditional technology (failover-type) testing as opposed to testing the recoverability from for example a cyber disruption event which requires additional consideration.

In addition to the testing proposed, we would support 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 to firms and FMIs on an annual basis.

For all types of testing, an impact assessment of risks identified must be done in conjunction with the consumers of the CTP as the severity will differ dependent on consumption of the service.

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

For the reasons set out at Q16, AFME strongly supports the proposal for CTPs to share certain information with firms. While recognising the confidentiality concerns of providers, access to key information will only bolster the operational resilience of the sector and ensure that FIs are less likely to caught off-guards by risks which are not directly within their own view or control. The focus on sharing lessons learnt / remedial actions from testing appears a sensible balance and will assist FIs in identifying information which is most impactful. We do however recommend that a RAG rating is applied to all such lessons

learnt/remedial actions so that financial institutions can efficiently assess which are most likely to have possible impact on them as client. Any such RAG rating should be accompanied with a key to provide financial entities with information on how the CTP has based its RAG determination/classification. The BoE should ensure that CTPs are required to share such information *without undue delay*.

We also appreciate that a summary of the annual self-assessment may be the correct balance for authorities to strike, in terms of information sharing versus safeguards for confidentiality and sensitivity. We do however stress that the summary should contain the following information:

i. An overview of the key external and internal risks identified under Requirement 2: risk management, including the financial resilience of the CTP itself, and specific breakdown of key risks per material service.

ii. Any identified risks, including concentration risks, associated with supply chain management under Requirement 3, as part of the CTP's due diligence assessments, limited to the key Nth party service providers.

iii. Any materialised risks which required remediation as part of any changes to the CTP's own obligations on Change Management under Requirement 5.

iv. Consolidated information on subcontracting – this would streamline existing processes whereby many firms ask for this information bilaterally, improving efficiency and consistency for both CTPs and FIs.

v. Information on the CTP's strategy for the coming year(s), in particular any planned changes in relation to material services.

vi. Information on the CTP's Continuity of Business preparedness and testing.

We additionally seek clarification on how FIs will be informed of any recommendations made by authorities in response to a CTP's annual attestation, for example to further redress any risks which are identified. It is our assumption that the annual assessments will be subject to monitoring by the authorities and are unclear how this can be factored into an FI's risk management policies in a proportionate and consistent manner.

Finally, in addition to i) lessons learnt/remedial actions from testing and ii) a summary of the annual self-assessment, we strongly recommend that the Financial Sector Incident Management Playbook is made available to financial institutions.

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

In the 2022 discussion paper it was acknowledged by the UK authorities that there were limitations from the existing regulatory framework, including that FIs are unable to assess system-wide concentration and that this could pose a potential systemic risk. The information gathering provisions of the incoming regime will assist authorities in having proper sight over such risks in the future. Yet the most appropriate response from

authorities will typically be ensuring that any identified risks are captured within the risk management policies of either the CTP or the FI, or potentially both. This is especially the case given that in the field of financial services it will often not be feasible to seek to remedy such risks through substituting or eliminating parts of the supply chain. In order for FIs to do so they must be in possession of at least the summarised findings from the annual assessment (as outlined above).

We also reiterate our view that information received on CTPs will enhance and better inform decision making and risk management by the FIs. Each FI will be using a third-party provider and its services in a different manner, with different associated risks, and so they are best placed to determine how to respond. The sharing of information between CTP and FI will ultimately enable a more informed approach to due diligence.

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?**

As stated above, by proposing a summary of the annual self-assessment and to focus testing disclosures on remedial actions, we feel authorities are striking the correct balance. An additional mechanism, as proposed under the EU's DORA, would see the BoE produce annual collective recommendations for FIs, on the basis of their oversight of CTPs.

No further safeguards are proposed.

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?**

AFME previously voiced our concern that CTPs may seek to present publicly their designated status as a form of quality assurance or kitemark. We are therefore supportive in principle of this prohibition, though acknowledge there have been questions around enforceability.

Related to this, we stress that financial institutions should **not** be pressured into using a CTP over other providers.

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

As outlined in our response to the 2022 discussion paper, AFME is concerned that the regime could unintentionally exacerbate concentration or competition risk. We flag:

- There remains a degree of concern that when rolling out a new service a CTP may choose to limit FIs' access to that service in order to avoid the service being within the scope of the CTP regime and consequently subject to enhanced resilience requirements, at least until adoption reaches a greater scale.

- The cumulative resourcing burden proves increasingly unsustainable, for both CTPs and FIs, leading to higher costs of doing business.

- Should some CTPs decide to raise service fees, to cover compliance costs, that FIs coalesce around other providers, thereby increasing concentration risk and potentially barriers to market entry.

- Any regulatory push towards CTPs would further enhance concentration risk and curtail firms' flexibility to choose providers as best fits the firm's operating model.

We would again recommend that the designation process allows a sufficient window between a TPP being notified they are at risk of designation and subsequent HM Treasury determination, with TPPs who intend to withdraw from the market permitted an adequate grace period before they must cease providing services, in order to enable FS firms to execute relevant exit/contingency policies as necessary. While acknowledging that CTPs will have 12 months after designation to complete the identification and documentation of resources, there appears no clarity on timeframes for designation itself. We recommend that the BoE seek to synchronise with the parallel developments which are ongoing in the EU with DORA and the US with the bank Service Company Act (BSCA).

Finally, the approach to substitutability in a forced exit scenario also needs to be thoughtful. Forcing CTPs and consumers to the lowest common denominator level of service\capabilities to mitigate operational resilience risk could result in unintentional increased risk. For example, requiring firms to support delivery of their value chain through multiple CTP providers could increase risk of production incidents due to increased complexity in a dual vendor configuration versus single vendor. The possibility and level of substitutability should be captured within a CTP's exit scenario testing, with CTPs required to flag if they feel there is no possible substitute at all.

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

We would flag that the costs to financial institutions from setting up the CTP regime have not been fully appreciated in the cost-benefit analysis. While the analysis acknowledges that CTPs may in due course seek to pass on the costs of compliance to firms as clients, the upfront costs to financial institutions have been overlooked. Despite assurances from authorities that CTP designation should not impact the responsibilities of firms, it is almost inevitable that there will be an increased burden, especially in the initial phases where providers remain beyond the regulatory perimeter.

Contacts

AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@afme.eu
AFME	Coen Ter Wal	+44 (0)20 3828 2685	coen.terwal@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/