Consultation Response

DP22/3: Operational Resilience*: critical third parties to the UK financial sector*

21st December 2022

Executive Summary

AFME welcomes the opportunity to respond to the Joint Discussion Paper by the Bank of England (BoE), Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) (the authorities) into ***Critical Third Parties to the UK financial sector***[1].

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.

The regulatory direction of travel to provide for direct oversight and supervision of certain Third Party Providers (TPPs) was anticipated and we welcome the level of dialogue from officials which has accompanied this consultation. The Discussion Paper provides important initial insight into how the authorities will use new powers under the Financial Services and Markets Bill.

To ensure a regime which we believe best fulfils the ambitions of the UK authorities, we have identified the following four overarching principles:

1. **Focus on risks which are truly systemic, as opposed to all TPP services which support the Important Business Services (IBS) of Financial Sector (FS) firms.** We acknowledge that the creation of a framework for TPPs designated as 'Critical' has the potential to achieve real benefits, including advanced sight of third party vulnerabilities. Success though depends on authorities carefully targeting only those services where disruption would have a systemic impact within the relevant FS firms. We caution against a number of the proposals within the Discussion Paper which could lead to a significantly higher number of CTPs than anticipated. This would cut across existing or incoming regulatory frameworks, creating conflicting misalignment and driving up costs.

2. **Avoid unintentionally exacerbating the underlying concentration risk that authorities are seeking to address.** We recommend that authorities streamline the incoming regulatory requirements by: taking account of existing voluntary certifications; mutual recognition of testing which is undertaken by non-FS authorities or authorities in other jurisdictions; and ensuring sufficient windows between resilience exercises to enable remedial action. A resource-intensive framework could

[1] Bank of England, DP3/22 – Operational resilience: Critical third parties to the UK financial sector, 21 July 2022, https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector

deter TPPs from providing services to FS firms. This would accentuate the underlying concentration risk, especially with regards to Cloud Services.

3. **Greater clarity is needed on the ongoing role for FS firms in both identifying TPPs for designation and enabling them to implement the minimum standards.** AFME strongly endorses the intention to align the framework for CTPs with the operational resilience requirements currently in existence for FS firms. It ensures familiarity and reduces regulatory inconsistency. We include for reference a series of proposals which we believe will assist authorities in designing how the framework should work in practice. Authorities should be directly leveraging information which is already available rather than issuing new data requests. There is particular concern over the proposed mapping obligations and how the Financial Sector Continuity Playbooks (FSCP) will be maintained.

4. **CTPs should remain responsible for complying with all their obligations under the proposed oversight regime.** AFME members want sight of any identified CTP vulnerabilities, from either live incidents or testing, to factor into their own risk management. This should not, however, creep into an expectation that the FS industry acts as supervisor of CTP compliance or is responsible for enforcing actions identified from live incidents or testing exercises. If remedial action is required, due to lack of adherence with the standards, authorities should be seeking corrective measures from the CTPs.

Finally, as acknowledged within the Discussion Paper, we wanted to recognise that there is a significant amount of international interest in this topic, and a growing concern amongst AFME members of a fragmented and duplicative set of regulatory demands upon multi-national FS firms. For this reason we recommend a mixture of operational coordination between authorities, and alignment of regulatory approaches. We have included within question 16 below a set of principles[2] on which this could be based, developed by AFME's global affiliate GFMA, with its international remit.

Given the level of interest in this consultation we have responded to each of the questions within the Discussion Paper and we remain available to discuss any of the specific answers in further detail.

Consultation Questions

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

   The wider digitalisation of financial services brings with it a range of benefits including speed of service, scalability of products, greater transparency and enhanced accessibility. Many of these benefits have become widely demanded by clients and regulators alike but have required a level of technical innovation which is often only possible through the commissioning of TPPs.

[2] GFMA, Proposed GFMA principles regarding Critical Third Parties, June 2022, https://www.gfma.org/wp-content/uploads/2022/06/proposed-gfma-principles-regarding-critical-third-parties.pdf

It is welcomed that the Discussion Paper explicitly recognises the benefits which are realised through the role of TPPs. The Discussion Paper notes how the implications of this trend have spurred various reviews and reports, both at the UK level, through the Kalifa Review and in the reports of the Financial Policy Committee and the Treasury Select Committee, and at the international level, by the Financial System Stability Assessments of the International Monetary Fund. AFME fed into a number of these reviews and does not object in principle to the overall finding that reliance upon TPPs brings with it a number of new risks.

AFME agrees that the potential impact on broader market stability and integrity stems from the underlying concentration risks, through either multiple direct contractual arrangements or indirect interconnectedness (i.e., supply chains). This results in overall dependence on a limited number of suppliers, with the market most condensed in the provision of Cloud Services Providers (CSPs). We stress, however, that disruption to the provision of a third party service, even a major provider supporting an Important Business Service (IBS) of a FS firm, is not necessarily of itself a systemic risk. AFME strongly advocates a targeted approach to risk management, focused on those risks which are truly systemic.

AFME also stresses that authorities should recognise upfront how TPPs may already be subject to non-FS specific oversight or regulation. A prime example would be where the Security of Network and Information Systems (NIS) Regulations 2018 are in force. Recognition of, and alignment, with existing frameworks will be critical for avoiding regulatory overlap and operational friction. Similarly, given the existing operational resilience requirements already in place for FS firms, we would additionally call for a specific exemption for FS firms' intra-group providers (i.e., where part of the group supplies services to others in the same group), including those that are regulated and supervised by non-UK authorities. To treat intra-group providers, including those based overseas, in the same way as TPPs would fail to recognise the operational differences, including the higher degree of control and oversight under which they operate. We would welcome the latter exemption being clearly articulated in the rules. In addition, we understand that the intention of the authorities is that FS firms that are regulated and supervised by non-UK FS authorities are excluded from being designated as CTPs and we would again ask the authorities to explicitly set this out in the forthcoming consultation paper and subsequent rules.

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

AFME members have welcomed the degree of openness and level of dialogue which the joint team at BoE/PRA/FCA has provided, along with officials at HM Treasury. It has enabled AFME members to anticipate the proposed extension of the regulatory perimeter. It is not possible for a single FS firm or FMI to assess system-wide concentration. As the authorities' current powers in general only allow them to impose requirements and set expectations on FS firms, FMIs, and certain parent undertakings, this is an apparent shortcoming. AFME does not object to the conclusion that the authorities currently lack the power to compel action from TPPs in the way that currently exists over FS firms.

We are also conscious that a number of international authorities share the same conclusions of the UK authorities, in particular EU authorities who are likewise proposing an extension of the regulatory perimeter within the Digital Operational Resilience Act

(DORA)[3]. The focus on *critical* third parties is a growing trend across jurisdictions, with some already implementing measures to enable this (e.g., EU, South Korea). There is though a worrying potential for various international regulators to take divergent approaches in responding to this conclusion. We develop this concern later in our consultation response.

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

   AFME endorses the focus on minimum standards and resilience testing, as a way of ensuring a principles-based and outcomes-focused approach. To be more prescriptive, or set out specific technical requirements on certain functions, risks creating a framework which could stifle innovation, quickly become out of date, or create misalignment with the existing operational resilience framework already in place for FS firms. This last factor is one of the key concerns of AFME members. Member discussions have raised widespread concern over the potential for misalignment, duplication and corresponding in-efficiencies across the Discussion Paper's proposals and we expand on specific issues later in the response.

   Additionally, CTPs could be subject to non-financial and non-conduct aspects of the Principles for the Sound Management of Operational Risk (PSMOR) and aspects of the Senior Managers and Conduct Regime (SMCR). Such requirements would assist with the proposed alignment discussed in question 4.

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

   The intention to align the framework for CTPs with that already in place for FS firms is a particularly welcome proposal within the Discussion Paper and helps directly address the primary concern within AFME's members over misalignment between the two sectors. A mirrored framework has the advantage of familiarity, enabling a better understanding which will assist in the embedding and implementation of the framework within the FS industry. It also increases the opportunity to identify and secure increased efficiencies, which may help mitigate the anticipated additional costs facing FS firms who are seeking to do business with CTPs, for example by enabling the leveraging of existing data and information. Given the relatively small number of CTPs expected to be nominated, it would likely be disproportionate to increase the reporting burden across the industry to identify services which may already be identifiable based on existing data reporting by firms, publicly available data and data held by other authorities such as the Competition and Markets Authority (CMA). Further thought is set out in the next set of questions, but such leveraging will be key to unlocking the potential regulatory efficiencies and preventing duplication.

[3] European Commission, Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector, Brussels, 24.9.2020 COM(2020) 595 final

Any alignment must capture underlying assumptions, including the recognition that disruption to systems will occur. Critically it must also encompass alignment in practice, including definitions, terminology, and processes. There is concern around the potential misalignment in some of the core facets of the framework, for example what is considered to be *systemic* or what is defined as a *material service*. We are particularly concerned about misalignment between the *material services* identified by CTPs versus the IBS of FS firms. CTPs must not regard all services which support a FS firm's IBS as material, but instead tailor such mapping around systemic risks and subject to meeting a certain threshold which is proportionate to and suitable for the CTP's operating model. The approach to material services should also be consistent across CTPs and a common service taxonomy provided in order to ensure consistency.

AFME expects the framework for CTPs to develop over time, and to build upon the outlined standards. The authorities should look to establish a formal review process for this framework, as in the absence of formal review mechanisms, the two frameworks may diverge over time. If such formal reviews were to be conducted, they should assess the broader spectrum of obligations relating to operational resilience, identifying opportunities for rationalisation. By focusing narrowly upon those services of CTPs which truly pose a systemic risk, authorities would mitigate the potential for divergence.

AFME flag here further ambiguity in how the proposed framework will work in practice and would welcome clarification on:

- How will HM Treasury notify FS firms of the designated CTPs?
- Will either the authorities or HM Treasury publish and update the list of CTPs? Alternatively, will CTPs notify FS firms?
- What will be the frequency of the review of determining whether a third party meets the CTP designation criteria?
- How will the authorities apply this regime to third country CTPs?

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

It is noted that the Discussion Paper states that by focusing on materiality and concentration, "*CTPs are likely to comprise a very small percentage"* of the total number of third parties providing services to FS firms. We agree with this assessment. A targeted and concise regime will be key to ensuring that the costs, processes, and resourcing are proportionate to the end outcome. A regime with hundreds of CTPs would be difficult to manage and would exacerbate the risk that there is not a targeted focus on truly systemic risks. Further clarity would be welcomed on whether there are any parts of the third party supply chain which are of particular focus, or conversely considered out of scope, and whether the authorities will treat ICT CTPs differently from non-ICT firms. AFME members would flag that in practice, it may be difficult for CTPs to identify and ringfence which of their services are used solely by FS firms.

There is additionally a degree of uncertainty over how the outlined criteria align with other legislation which may overlap. For example, the *systemic impact* definition/test within the

Materiality criteria compared to that within the parallel HM Treasury consultation on the Payments Regulatory Perimeter[4]. Alignment will be key to avoiding future confusion.

AFME members did not have any further suggestions to consider as part of the designation process.

6. **What are your views on the supervisory authorities' potential approach for assessing concentration, materiality and potential impact in the provision of third party services to firms and FMIs? Are there alternative approaches for doing so that could be more effective or pragmatic?**

The Discussion Paper makes clear that the implementation of the proposed approach to designation requires a significant level of input and resourcing from FS firms:

- The assessment of *Materiality* will be based upon the *overly broad* economic functions listed within PRA SS19/13[5]; the critical functions within s3 of the Banking Act 2009[6] and certain IBS as defined in the Operational Resilience Policy Statements[7].
- On *Concentration*, the authorities will be seeking to establish direct dependencies, indirect interconnectedness, and the *constantly evolving* market share.
- We understand FS firms' business continuity plans, exit plans and scenario testing are expected to be part of the assessments on *Potential Impact* (aggregation risk, substitutability and survivability).

AFME would welcome clarity on how to put these obligations into practice. Certain elements of the proposed data and information are already available to supervisors through the existing operational resilience requirements on FS firms. We would encourage the authorities to leverage this existing reporting and other external data sources (such as publicly available information from the Outsourcing Registers, and data held by other authorities such as the CMA). Notwithstanding the broader *Transforming Data Collection* programme, AFME members remain highly concerned that authorities will instead issue new, duplicative data requests. There is further concern that authorities will seek information from FS firms on Fourth Party Providers and/or other subcontracting counterparties beyond the original TPP. Given FS firms have little power or ability to compel TPPs to disclose this information, or more commonly to ensure that they respond with the level of detail expected, the authorities should seek this information directly from the TPPs or CTPs.

In terms of the specific designation criteria, we recommend that:

[4] HM Treasury, Payments Regulation and the Systemic Perimeter: Consultation and Call for Evidence, https://www.gov.uk/government/consultations/payments-regulation-and-the-systemic-perimeter-consultation-and-call-for-evidence

[5] Prudential Regulation Authority, Supervisory Statement SS19/13, Resolution Planning, June 2018, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2018/ss1913-update.pdf?la=en&hash=AF6C017CD36D5EE06321E150441D185252D97065

[6] Banking Act 2009, EW, s3

[7] Prudential Regulation Authority, Policy Statement PS6/21, Operational resilience: Impact tolerances for important business services, March 2021, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2018/ss1913-update.pdf?la=en&hash=AF6C017CD36D5EE06321E150441D185252D97065

- Firstly, authorities more narrowly construe the *Materiality* criteria to both ensure greater alignment with the framework for FS firms and achieve the advocated focus on systemic risks.
- Secondly, authorities should clarify how they will calculate the market share of TPP services, given this will continuously evolve within the changing landscape of the market.
- Thirdly, the authorities develop a set of parameters, based upon alignment with FS firms' IBS mapping, to provide further guidance on the *Potential Impact* criteria.

AFME would also call on the authorities to expand on the proposed methodology in determining whether to recommend designation having assessed a TPP against the above criteria. Without such a collective threshold, designation would capture too wide an array of TPPs, thereby failing to ensure a tight focus around only those which pose a systemic risk. This is a growing concern, given the varying potential for providers to meet the stated tests across the criteria. For example, a provider could meet the *Economic Functions* test as part of the *Materiality* criteria, but not the *Critical Services* or *Systemic Impact* tests. Would such a provider therefore have to meet a higher threshold under the *Concentration* and *Potential Impact* criteria? Alternatively, are any of the criteria seen to be triggers or a tipping point, for example around *Substitutability*?

The Discussion Paper notes that any of the three authorities could recommend designation to HM Treasury, subject to a Memorandum of Understanding (MoU) on coordination. A clear and transparent process for designation, based on uniform criteria, will be critical to avoiding: a) the potential scenario of a TPP being deemed critical by one of the authorities but not the others, due for example to the differing remits of each (i.e., the FCA's broader consumer scope compared with the PRA); and b) FS firms being obligated to provide data to more than one supervisor at the same time due to parallel ongoing reviews.

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

AFME endorses the proposed ambitions on aligning cross sectoral linkages including through formal means such as MoUs. The concern is that without formal coordination non-FS authorities may decide to address the same risks or obtain the same information as covered by this proposed regime. That could lead to duplication, inconsistencies or even unintended consequences.

To avoid the above risk, we would urge authorities to agree formally amongst themselves how they will share the data captured through the CTP framework and how they will notify in advance any regulatory intervention. This should ensure that if the Information Commissioner's Office (ICO) or another non-FS regulatory body needs the underlying information, they are able to obtain the same set of data, enabling aligned benchmarks and databases across sectors.

8. **What are your views on how best to avoid or mitigate potential unintended consequences, including potential distortion, such as deterring third parties from**

entering the market or providing services to firms and FMIs, as a result of a third party being designated as a CTP?

Any policy intervention carries with it the risk of unintended consequences. As a general position AFME has long supported the need for outcomes-focused and proportionate regulation as one of the key overarching ways in which to mitigate against these risks. The Discussion Paper aptly calls out the risks on choice and competition for FS firms, should third parties be deterred from providing services to the sector. This remains a concern for the industry, and includes the risk that CTPs may delay the availability of services to FS firms. For example, when rolling out a new product a CTP may choose to limit FS firms' access to that service in order to avoid the product being within the scope of the CTP regime and consequently subject to enhanced resilience requirements, at least until adoption reaches a greater scale. Such an eventuality would in fact exacerbate the underlying concentration risk as FS firms shift onto a falling number of TPPs.

We also flag as other potential unintended consequences:

- The cumulative resourcing burden proving increasingly unsustainable, for both CTPs and FS firms, leading to higher costs of doing business.
- Market participants wrongly viewing designation as a form of quality assurance or kitemark.
- Should some CTPs decide to raise service fees, to cover compliance costs, that FS firms coalesce around other providers, thereby increasing concentration risk, and undermining regulatory aims.

While AFME welcomes the intention to avoid unintended consequences we are of the view that it would be better to provide margin for their occurrence. We would therefore 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. Developing case studies with potential CTPs on the implications of designation, stressing the risks at play, could also help signpost at an earlier stage any unintended consequences.

AFME members also recognise that there are potential unintended consequences which may have a benefit for FS firms. The creation of regulatory obligations upon CTPs could be an important first step in ensuring a greater alignment of objectives and incentives between the two sectors. This may need to be further addressed in future, potentially through a Shared Responsibility Model, whereby regulatory responsibilities are more evenly balanced between CTPs and FS firms.

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

The view amongst AFME members is that the standards are familiar in rationale and coverage. AFME strongly endorses the outcomes-based approach, and we welcome the intention to align with the operational resilience framework for FS firms. We have specific comments on four of the proposed standards:

- *Identification of material services*: Given that the FS authorities have to date not regulated CTPs, it is possible CTPs may not be familiar with the statutory objectives under review. CTPs should consequently not be identifying their *material services* in isolation, but in conjunction with the authorities, who are the only entities with cross-market perspective over concentration and other systemic risks, and who should ensure the CTP *material services* are correlating accurately with the IBS of FS firms. While a service may be deemed material or critical/important at the system level, this does not automatically mean it will be at an individual firm level. An FS firm should have the ability to overlay a CTP designation based on the engagement it has with that CTP. Based on current reading there are differing views as to whether firms should or can take responsibility for informing CTPs with whom they contract, which of their services support which IBS, partly driven by the fact that direct engagement with TPPs by the authorities may be more appropriate. There was unanimous view however that FS firms should not be responsible for validating the identification of *material services* by CTPs, and that the authorities should explicitly provide in the final rules that CTPs are fully responsible and accountable for complying with all of their regulatory obligations and that they will not be able to delegate any of their responsibilities to FS firms.

- *Post-incident communication*: We are keen to hear more on how CTPs would co-ordinate with FS firms as part of the Post-Incident Comms Plans, with clarity over who will communicate what information in different circumstances (for example live incidents versus resilience exercises). Authorities should explicitly state expectations for CTPs on communication and cooperation, in order to reduce potential frictions in interpretations which may deprive the new CTP regime of tangible benefits. We are conscious that Post-Incident Comms Plans are also aimed at mitigating the risk of an incident becoming systemic, for example through a bank run, and therefore immediate reactions may be required from AFME's members. To that end, CTPs could be required to establish a designated senior representative to attend CMBCG (Cross Market Business Continuity Group) and FSCCC (Financial Services Cyber Collaboration Centre) in the event of an incident. The information they would be expected to provide could be adapted from the UK's existing Principles for a Paralysed GSIB and the Reconnection Framework. Members have also indicated the guidelines within TARGET 2 as a useful template in this regard.

- *Financial sector continuity playbook*: Likewise, we would welcome clarity on the expected involvement by firms on the development and testing of the FS Continuity Playbooks (FSCP). While welcome, this has the potential to be highly complex to create, test and maintain, and may require substantial collaboration. To avoid this quickly becoming overly burdensome, we recommend developing Best Practice guidelines through Public-Private bodies such as the BoE's CMORG (Cross Market Operational Resilience Group).

- *Learning & evolving*: Of particular interest to AFME is the standard on *Learning & Evolving* and specifically the requirement on CTPs to extract lessons from a live incident or any testing exercise and share these with relevant FS firms. This could prove highly beneficial in providing the FS industry with advance sight of potential vulnerabilities and risks which they will consequently be able to factor into their own operational resilience planning. One of the key questions to supervisors is whether the scopeis limited to firms with a contractual relationship? AFME believes there would be benefit in greater visibility, in order to provide warning to FS firms who may be planning to enter contracts with the relevant CTP. Secondly, while members welcome sight of potential CTP vulnerabilities, and may respond to these within their own operational resilience risk management frameworks, it would clearly be inappropriate for FS firms to ensure that the CTPs have rectified their potential

vulnerabilities. This role sits firmly with the authorities. Members have noted that CTPs are not subject to a Senior Managers and Certification Regime (SMCR) equivalent governance regime. Without clear and specific governance requirements, there are likely to be issues in embedding the lessons learnt properly. The authorities should set out explicit approval and governance requirements as part of the CTP resilience framework. Developing the *Learning & Evolving* standard and ensuring it is fully utilised and leveraged would directly impact the need for other transparency mechanisms, such as the Ratings system which authorities propose later in the Discussion Paper.

We understand it is possible the resilience standards may be applied at varying levels, depending on the potential impact to the FS sector. It may be that certain parts of the third party supply chain (for example CSPs) are in practice likely to attract greater attention by the authorities, as suggested within question 5. If CSPs, for sake of illustration, are subject to a heightened application of the standards, this should remain outcomes-focused, for example around major or prolonged outages. The smaller the number of CTPs, the more likely a uniform application of the standards is feasible.

Please note, we cover member views on testing in the questions 12 – 14. Question 12 also includes AFME thinking on the monitoring and enforcement of CTP compliance with the minimum standards, in absence of specific questions on chapter 7 of the Discussion Paper (*supervisory authorities' use of proposed statutory powers over CTPs*).

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

AFME has concerns that international regulators and bodies are pursuing separate and disjointed strategies in this field, despite the cross-border nature of many TPPs and the risks associated with them. While AFME welcomes the UK approach, there is potential for divergence, even with regards to the EU's DORA despite alignment of overall objectives. The main concern within industry is a growing plethora of schemes, standards or certifications which are all purporting to address the same risks. Application at jurisdictional level will create a patchwork of obligations and ultimately this will not serve the overall resilience of the sector. Additionally, while investment in operational resilience, and especially digital resilience, remains a priority for industry, efficiencies are critical to ensure that allocated resourcing achieves maximum potential. Where possible, if TPPs have obtained a relevant certification in one jurisdiction/market, whether voluntary or mandatory, this should be considered in other jurisdictions/markets.

This is most clearly visible in the Cloud and Cyber sectors, where the number of schemes, predominantly voluntary, continues to grow. The Discussion Paper notes several international examples. In addition to these we would flag the EU Cybersecurity Certification (EUCC) and the EU Cloud Certification (EUCS), along with the other schemes under development by the European Union Agency for Cyber Security (ENISA).

More generally, we support the ambition for global harmonisation, however note this does not in itself limit the risk of duplicative certifications. To avoid duplicative schemes or certifications emerging, we advocate a broader, outcomes-focused approach when considering whether to formally recognise existing schemes, rather than seeking direct homogeneity.

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

As mentioned above, AFME is very aware of the implications for FS firms in the adoption of the stated standards, especially the level of input and engagement in the creation of the Financial Sector Continuity Playbooks, the coordination on post-incident communication, and through the response to any lessons learnt from live incidents or resilience testing. This will require additional resourcing and incur higher costs, yet there remains willingness to facilitate further collaboration between CTPs and FS firms, for example on the identification and mapping of material services. We note though that under section 7.2 of the Discussion Paper, the authorities may ask FS firms in response to the above standards on CTPs, to enhance their due diligence, monitoring, or business continuity and exit plans for any material services they receive. This has raised concern over whether authorities will impose new requirements on FS firms which receive services from CTPs in addition to those existing under SS1/21 and SS 2/21[8]. Our members' view is that regulatory requirements currently applicable to firms and the contractual arrangements with their TPPs are robust and fit for purpose. There is no added benefit in creating new obligations or requirements to continue usage of a CTP. The authorities should instead continue to support a risk-based approach to third-party oversight by firms.

From a FS firm's perspective, any information received on CTPs should serve to enhance and better inform decision making and risk management. The proposed CTP regime, if effectively implemented and coordinated across jurisdictions, could also provide firms with useful information to supplement existing due diligence practices. Firms should remain able to leverage their oversight frameworks with any intelligence received, whether from regulators, their own due diligence, pooled audits, or third party audit reports, to help inform firm-level decision making and potential impacts. In this regard, it should again be acknowledged that a third party service deemed material by the UK authorities at the system-level should not automatically mean that it is material or critical for an individual FS firm, nor should one-size-fits-all actions be mandated of FS firms from such a designation. Each FS firm will be using a third party and its services in a different manner, with different risks associated with those different usages. For example, data use, data volume and the importance of the service to a particular FS firm are some of the aspects factored into the criticality rating of a third party arrangement. It is therefore important that FS firms remain responsible for determining which actions they would require a CTP to take in order to address its specific usage. Ultimately, the result of the CTP regime for FS firms should not be seen as automatically requiring more due diligence, but a regime enabling a more informed due diligence approach by FS firms with designated CTPs, in the context of an FS firm's specific service usage.

This also raises the issue of how to monitor and track CTPs' adherence to the minimum standards. The understanding is that this will be based upon a CTP's internal annual self-assessments, in line with the approach adopted with specified service providers to payment systems. Considering the concerns referenced above, over the disparity in governance between FS firms and TPPs, AFME would recommend that the self-attestation requires further consideration but would also not recommend that this responsibility is transferred onto the FS sector. Further, any material action which stems from a CTP's failure of compliance should be determined and implemented by the CTP, as soon as it becomes aware it is in breach of its regulatory obligations under the new regime. Remedial action by

[8] Bank of England, Supervisory Statement 2/21, Outsourcing and third party risk management, https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss

the FS firm should only be sought in the event the CTP has demonstrated it is unable to resolve matters.

AFME additionally makes four recommendations to help mitigate the costs of complying with the minimum standards:

- Leverage existing data and information which is already available to authorities rather than calling on CTPs to issue new data requests.
- Avoid misalignment between the framework for CTPs versus FS firms to help limit costs. The suggestion that the CTP framework will evolve overtime causes concern about longer term divergence.
- Review the potential for non-mandatory model Standard Contractual Clauses (SCCs) in the provision of third party services, limited to minimum requirements (akin to Art 28 GDPR or the ISDA Master Agreements within the OTC derivative market). If the authorities do propose SCCs, they should be narrowly tailored and aim to address specific pain points/areas of concern. For example, FS firms frequently receive pushback from service providers when negotiating key contractual provisions relating to the firms' access, audit and information rights, entitlement to participate in a service provider's Business Continuity Plan tests, termination rights and FS firms conducting penetration testing. SCCs could also include provisions on obtaining specific information from sub-contractors.
- Using a phased approach to implementation, with authorities spreading the implementation of requirements over time, minimising the impact to service costs.

More broadly, there is the question of costs for authorities in bringing this framework into practice, and how authorities will fund these costs. AFME strongly believes that regulatory costs should be fairly and proportionately shared by all including financial contributions from the CTPs. We remain wary though that CTPs could pass through these costs onto their FS clients.

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

AFME stresses a number of overarching factors that are key to making industry-wide resilience testing successful:

- Given that sector-wide exercises are resource intensive to organise and run, with potentially long-running requirements to address, they are most suitable to the highest-risk challenges facing the industry rather than as a method of assurance.
- The success of such exercises, including both the exercise itself and the follow-up actions to address identified weaknesses, depends on the willing engagement of the CTP. If viewed as a compliance or tick-box exercise by the CTP, then the chances of meaningful progress are reduced, and timelines are likely to extend.
- Tailoring realistic scenarios to the CTP is essential to identifying real weaknesses or areas of further exploration. We are conscious of industry exercises based on scenarios that the participants did not consider realistic, or which were simply too large to allow for the identification of specific weaknesses. For example, past exercises designed around the complete failure of a major CSP have not been successful in generating the desired results.

The UK authorities could consider other forms of industry resilience testing, such as industry-led business continuity exercises (i.e., tests extending beyond table-top exercises). Such tests can be effective at strengthening preparedness for targeted areas of cyber response. Examples include SIFMA Classic[9], Reg-SCI[10] and FIA[11], all of which are designed to exercise FS firms' capabilities to failover from their primary to secondary sites, as well as other elements of the business continuity playbooks. Two elements distinguish these exercises and make them useful models for future CTP exercising regimes:

- The exercises test actual ability to maintain market services; and
- The tests ensure that FS firms are present, retain high level understandings of the outcomes of the testing and engage in information exchanges regarding respective resilience capabilities.

While not necessarily suited to CTPs, such testing could serve as an example of how resilience can be exercised between key partners in a collaborative and open way.

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

AFME welcomes the recognition within the Discussion Paper that the level of resourcing demanded by each of the resilience testing tools varies and that sector-wide testing in particular entails a significant level of resourcing, coordination, and time. This has led to the international tendency to set such exercises every three years, which AFME agrees is the right continued frequency. We would urge that in order to keep the costs feasible, any sector-wide exercise encompassing CTPs should be built into existing initiatives, such as the Bank of England's SIMEX simulation driven by the Cross Market Operational Resilience Group (CMORG). The secretariats for these existing programmes would naturally be expected to take primary responsibility for monitoring the recommendations from such an exercise. For the same reason, the proposed reliance on CTP scenario testing as the most frequently used tool, due its resource-effectiveness and versatility, is a welcome approach. AFME would like to flag however that experiences to date indicate further guidance is needed as to what amounts to "*severe but plausible*."

AFME notes that the main implication for FS firms from the CTP framework is the proposal for sector-wide exercises, which includes joint testing between CTPs and FS firms. AFME welcomes this collaborative approach to resilience testing and many of our members are already working closely with their TPPs to this end. Our view is that joint testing can enable the FS industry to have first-hand transparency and greater understanding over supply chain risks which could threaten operational resilience. Collaboration in testing also helps mitigate the risk of unintended consequences, by ensuring that TPPs and their clients can test risks and solutions in partnership. Our concern is that the level of resourcing demanded for resilience testing is growing on two fronts: firstly, there is the expectation to undertake

[9] SIFMA, Securities Industry Business Continuity Test, 15 October 2022, https://www.sifma.org/wp-content/uploads/2022/07/2022_Industry_Test_Overview_Start.pdf
[10] SIFMA, Reg Sci Playbook, Oct 2021, https://www.sifma.org/wp-content/uploads/2020/04/SIFMAs-Reg-PlayBook-v.10192021.pdf
[11] FIA, FIA Disaster Recovery Exercise, 15 October 2022, https://www.fia.org/fia-disaster-recovery-exercise

additional tests, in conjunction with a wider array of non-FS and non-UK partners; and secondly, that each test is itself becoming more intensive and resource demanding. The cumulative burden of this trend is an increasing concern for AFME and requires action from authorities. In this regard, AFME would call for greater mutual recognition of testing, across the two UK frameworks and indeed across other markets. By this, any joint testing with CTPs should be considered to meet existing operational resilience obligations on the FS industry, rather than in addition to exercises entailing only FS market participants. Similarly, we would like to see the PRA extend/clarify its principle of proportionality (under SS2/21) to allow firms to factor the existence and output of new CTP resilience testing when framing the level and scope of internal third party resilience tests against the same population of regulatory designated CTPs.

The proposed testing tools could include a requirement for collective exercises, co-ordinated centrally by each CTP and joined on a voluntary basis by relevant FS firms. This would form a pragmatic middle ground between individual functional/component testing and sector-wide exercises (where FS firms, FMIs and CTPs are equal players), with the established benefits of a "one to many" approach. We encourage the bundling of such an approach into existing schemes, for example initiatives overseen by the FSCCC or the Cyber Defence Alliance. Should FS firms opt-into additional testing, there would be a clear, and fair, expectation that any lessons learnt (*After Action Reports*) are fully shared, and that the FS firm be included in post exercise discussions.

Finally, members of AFME call for clarity on who will monitor the lessons learnt from testing and how they will track remedial action on an ongoing basis. Again, we are concerned that there is an expectation on FS firms to track how CTPs are complying with the recommendations from testing exercises. We have already noted above that FS firms should not be responsible for ensuring CTP compliance with the minimum resilience standards. For the same reasons, how recommendations from resilience tests are actioned should fall within the remit of the supervisors. This may be critical to ensuring that the investment in testing is fully utilised, especially considering the referenced concerns over CTP governance.

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

AFME members consider it unlikely that CBEST will materially improve the resilience of the largest TPPs such as the major CSPs. We see a minor risk in any regime which may result in those CTPs prioritising low or minimal risk findings over strategic priorities simply because those findings carry regulatory weight. Other potential risks, including the outsourcing of sensitive information to external testers, are set out in the 2020 paper on Penetration Testing published by our sister organisation, SIFMA[12]. The largest CSPs already offer the ability for customers to conduct Threat Led Penetration Testing (TLPT) on their deployments within the CSPs' environment. The value in such testing would therefore come

[12] GFMA. A framework for Threat-Led Penetration Testing in the Financial Services Industry, Dec 2020, https://www.gfma.org/wp-content/uploads/2020/12/gfma-penetration-testing-guidance-for-regulators-and-financial-firms-version-2-december-2020.pdf

from targeting applications which FS firms cannot already test. However, we believe that it is unlikely for the provider to be able to test their services in such a way that is specific to a single FS firm or the FS sector. Any risk generated by a CBEST test will therefore be relevant to all users of that service.

Conducting tests is resource intensive, including for the regulator. If the oversight regime is to include a significant number of CTPs, then a requirement to conduct CBEST tests is likely to present a significant resourcing challenge for the UK authorities. The lighter touch F-STAR may present an option for scaling the larger number of CTPs, but the decision to do so would largely be driven by resource constraints rather than a risk-based approach. The overall resilience of the sector would benefit from a more detailed and intrusive examination of the defences of a smaller number of the most critical CTPs than from a more cursory test of a wider number of CTPs.

From experiences to date, members have flagged that designing exercises specifically for CSPs carries additional difficulty. There are too many unknown elements of CSP resilience before moving to the level of complete failure in a most extreme scenario. We would that suggest authorities think about domain failures or which services are the most critical such that, if unavailable, they could impact other more systemic services ultimately leading to a broader impact. Authorities could also consider whether the mapping of such services should be included in the additional resilience requirements for CTPs. This could be an extension of the mapping suggested in section 5.9-5.10 of the Discussion Paper.

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

As stated above in relation to the minimum standard on *Learning & Evolving*, AFME welcomes granting FS firms sight of CTP vulnerabilities. The opportunity to factor these risks into firms' risk management controls and policies will strengthen not only their resilience, but also wider market stability. The challenge, as acknowledged in the Discussion Paper, is how to balance this transparency with confidentiality or market sensitivity considerations. In striking this balance, authorities must be alert to the risk of publishing data or setting up transparency mechanisms which are of little or no value to FS. The Discussion Paper suggests that ratings may be a way forward, but acknowledges how several existing ratings schemes in this field provide very high-level determinations: for example, *achieved*, *not achieved* or *partially achieved*. AFME does not support a similar approach to CTP resilience testing, due to a consensus that the value these provide is limited.

Members have expressed greater interest in refining and maximising how CTPs extract lessons from a live incident or a test and share these with relevant FS firms. This should provide more tailored insights and may mean any rating system would in any regards be duplicative. Before taking a firm position on this, members would like authorities to share

more clarity on the exact nature and content of information which will entail the minimum standard. Further clarity on the scope is also required, to understand which firms are likely to receive the extracted lessons. Our recommendation would be that supervisors take as much of a holistic approach as possible, on the basis of *Test Once, Share With Many*. In terms of refining and leveraging such information, we would also urge the authorities to obligate the CTPs to stipulate specific actions to follow an exercise, potentially in conjunction with FS firms. Additional regulatory guidance could shape the format of these extracted lessons, to ensure maximum value and that FS firms have transparency which is tailored around specific benefits. It is also highlighted that this is a further argument in favour of a regime based around a small number of CTPs, which would ensure a high quality of information is extracted and shared.

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

AFME welcomes the focus on international collaboration and stresses the need for harmonisation in regulatory approach and joined-up, coherent enforcement. The various international frameworks increase the risk of regulatory divergence, and we are especially concerned by the increasing duplication or friction through overlapping responsibilities or a lack of synchronisation. Members are particularly concerned that divergence will become entrenched in terms of Definitions and Terminology. There is, however, concern that a focus on global standards may struggle to achieve traction, especially considering the EU's developments through DORA which is now in its final phase. A focus on Global Principles, in tandem with standardisation of certain critical functions, for example on designation where the EU and UK approaches have a lot of similarity, is more feasible. AFME's global affiliate GFMA has developed and tested across a number of international markets a set of Principles for Critical Third Parties[13] which could be readily adopted. Longer term, any such Global Principles could be developed into Standards, but only should a relatively limited number of CTPs emerge globally, and this work is more appropriate for global bodies such as the Committee on Payments and Markets Infrastructures (CPMI), the Basel Committee on Banking Supervision, IOSCO (International Organization of Securities Commissions), or others, which have a demonstrable track record. Standardisation of third party risk management controls seems however particularly problematic, given differing approaches by regulators across the globe and could needlessly limit the freedom of FS firms to choose their own controls and take a risk-based approach.

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

One of the biggest issues facing multi-national firms present in various markets is the lack of sequencing between international regulators over the timing of resilience exercises. As the most resource-intensive tool, this issue is most impactful in the implementation of cross-border exercises. A simple recommendation would be the publication of the timings

[13] GFMA, Proposed GFMA principles regarding Critical Third Parties, June 2022, https://www.gfma.org/wp-content/uploads/2022/06/proposed-gfma-principles-regarding-critical-third-parties.pdf

for resilience testing of CTPs or the creation of a regulatory grid to ensure adequate sequencing. This may also highlight where duplication might exist across the various exercises. Sequencing of these exercises should provide a sufficient window of opportunity for FS firms and CTPs to enact the lessons learnt from past exercises before further testing is conducted. This would ensure an action and outcome driven approach to testing. Sequencing could also naturally develop into joint cross-border testing across multiple regulatory authorities. We urge regulators to coordinate on a bilateral level as well as on initiatives coming down from global bodies, such as the G7. We are aware that the UK authorities have already been working with the European Central Bank (ECB) and other EU authorities to conduct CBEST testing on a cross-jurisdictional basis, aligning with the Threat Intelligence-Based Ethical Red-Teaming (TIBER) EU framework. Such coordination provides the opportunity for regulators to compare and align testing techniques. In future, upon DORA coming into force, this could include participation with CTPs.

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

As with the resilience exercises within the UK, the form of cross-border testing which causes most concern amongst members is that of sector-wide exercises given their resource intensive nature. In order to address concerns AFME recommends that cross-border testing, when deployed, is a substitute for other testing/exercises. This could again be supplemented by the use of a voluntary, Opt-In approach for users of CTPs to additional cross-border testing. This would enable the larger FS firms with greater pools of resourcing to participate in further exercises.

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

There is a need for a harmonised approach across the different jurisdictions on the information that international regulators request and collect from FS firms via the outsourcing registers. There is currently a considerable degree of variation to the application of reporting requirements with FS firms having to maintain different outsourcing registers with different data points and formats. As part of the authorities' efforts to improve cross-border regulatory and supervisory coordination, authorities should work together to:

- Address the issues FS firms face with the current data collection processes; and
- Ensure the least possible divergence in the reporting requirements of the various outsourcing registers with the aim of creating a globally harmonised reporting model.

A harmonised approach will improve the quality and reliability of the information provided by FS firms on their engagement with CTPs, which will in turn help authorities with their monitoring of the CTPs' systemic impact on the FS sector.

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

AFME strongly encourages the UK authorities to recognise, where possible, overseas resilience testing undertaken by non-UK authorities. We see this as one of the most efficient ways of ensuring that resilience testing is resource-effective and that the shared desire by regulators to address the same underlying risks does not result in unnecessary duplication. AFME members would, however, like to receive further clarity on the *certain conditions* alongside recognition as referenced in the Discussion Paper question. AFME discourages against any move towards an international taxonomy, however it may be possible for regulators to seek Mutual Recognition Agreements with overseas authorities, building on bilateral MoUs, or to pursue similar commitments through global mechanisms, such as the Global Supervisory Colleges (the latter may prove a more receptive avenue in light of national regulators pursuing their own approaches to CTP testing). As an initial steppingstone, regulators should promote and secure regulatory recognition of any cross-border testing exercise which has input from a number of national regulators. In assessing the equivalence of such exercises, it will be critical to retain a focus on the outcomes of overlapping exercises rather than their precise conduct (with the possible exception of TLPT). AFME supports, for example, the Quantum Dawn[14] scenario testing on Cyber Resilience. This has been running for over a decade with engagement from US, EU and UK regulators, and participation from a CTP should be recognised as a valid joint testing exercise.

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

Given that CTPs may be subject to other non-FS regulatory regimes, and horizontal regulations such as the GDPR and the NIS Regulations, we encourage ongoing dialogue which facilitates industry input and engagement. This may prevent unintended consequences arising within FS from non-FS bodies intervening directly with the CTPs, notwithstanding existing MoUs and coordination through bodies such as the National Cyber Security Centre. One example is the potential divergence from the UK's Department for Culture, Media and Sports (DCMS) proposals on legislation relating to Cyber Resilience.

[14] SIFMA, Cybersecurity Exercise: Quantum Dawn V, 2021, https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-v/

Contacts

AFME	Andrew Harvey	+44(0)20 3828 2694	aharvey@eu.gfma.org
AFME	Ian Waterworth	+44 (0)20 3828 2685	ian.waterworth@afme.eu
AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@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/