March 15, 2024

Mr. Sam Woods
Chief Executive Officer
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA

Submitted via electronic mail

Re: IIF feedback on CP26/23 – Operational resilience: Critical third parties to the UK financial sector

Dear Mr. Woods,

The Institute of International Finance (IIF)[1] appreciates the opportunity to provide public comments to the Bank of England, Prudential Regulation Authority and Financial Conduct Authority, hereafter referred to jointly as "the UK Authorities", on Consultation Paper 26/23 on '*Operational resilience: Critical third parties to the UK financial sector*' ("the consultation").[2]

We have structured our feedback into overarching and thematic comments related to the consultation proposals, and specific responses to some of the consultation questions.

(i) Overarching comments

The IIF welcomes the UK Authorities' global thought leadership in the field of operational resilience. The IIF has engaged with several key global and jurisdictional consultations on operational resilience and critical third-party policy over the last several years since the UK Authorities first released their Discussion Paper[3] on operational resilience in July 2018.[4] The global financial industry continues to embrace the importance of operational resilience at the firm-wide level and with other key participants in the financial sector, and recognize the challenges

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks and development banks.
[2] "Operational resilience: Critical third parties to the UK financial sector". Also FCA CP 23/30.
[3] Bank of England, PRA, FCA (2018), "Building the UK financial sector's operational resilience".
[4] Including, IIF/GFMA (2021), "Priorities for Strengthening Global Operational Resilience Maturity in Financial Services" (hereafter, "IIF/GFMA 2021"); IIF (2021), "Response to FSB Discussion Paper on Outsourcing and Third-Parties"; IIF (2021), "Response to FSB Consultation on Third-party Risk Management" (hereafter "IIF 2021").

and potential risks of increasingly leveraging third party services to support their important business services. In a recently published 13th Annual EY/IIF Global Bank Risk Management Survey, operational resilience was ranked as the second-most urgent risk for the coming year by chief risk officers surveyed around the world.[5]

The IIF and our members have consistently advocated for a principles-based, outcomes-focused approach to operational resilience which is interoperable across jurisdictions and different regulatory frameworks and suited for financial institutions ("FIs"), financial market infrastructure providers ("FMIs") and the wider ecosystem.[6]

In recent years, a point that has been emphasized in IIF discussions on operational resilience with FIs/FMIs, the public sector, and other stakeholders is the growing importance of third-party outsourcing, particularly to Cloud Service Providers (CSPs). These outsourcing arrangements may be used, among other things, to gain entry to new markets, lower operating costs, fuel innovation and adapt to the evolving digital economy. Many FIs/FMIs have experienced the benefits of third-party outsourcing, for example as an enabler of digital transformation and enhanced resilience but are also cognizant of and managing the challenges and potential risks associated with such relationships. As the IIF has previously stated, the identification and provision of an appropriate regulatory framework for the operational resilience of critical third parties (CTPs) must be done by public sector authorities who have the necessary system-wide information and authority.

Given this, IIF members would like to express broad support for the UK Authorities' proposed principles-based regulatory approach to manage the potential risks to financial stability that may result from disruptions or failure at CTPs. The UK Authorities are helpfully proposing an outcomes-focused set of requirements which align with the current UK Authorities' operational resilience requirements for FIs/FMIs. Requirements to improve and oversee the operational resilience of CTPs will benefit the CTPs themselves, their customers, including FIs/FMIs, and members of broader society who use financial products and services.

The UK's proposed two-tiered approach to the CTP requirements, which distinguish between 'Fundamental Rules' and the more granular 'Operational Risk and Resilience Requirements' that would apply to a CTP's material services only, is an efficient way to focus efforts on the most salient potential sources of risk to financial stability. The proposed Fundamental Rules are sensible business procedures, which most third parties already strive to maintain.

The IIF supports the UK Authorities recognizing the importance of CTPs mapping their resources, including the assets and technology, used to deliver, support, and maintain each material service it provides,[7] and would expect all elements in the mapping (resources) to be subject to the CTP Operational Risk and Resilience Requirements. However, IIF members note that it is not expressly clear in the draft Supervisory Statement that the resources included in the mapping

[5] Tied with concerns about meeting regulatory rules and supervisory expectations. IIF/EY (2024), "13th Annual EY/IIF Global Bank Risk Management Survey".
[6] IIF/GFMA 2021.
[7] Requirement 6: Mapping, Section 5.31 of the draft Supervisory Statement.

would be subject to the CTP Operational Risk and Resilience Requirements. Additionally, IIF notes the mapping should be focused on the resources that are material to the delivery of the material service provided to FIs/FMIs; these could come both from assets and technology directly supporting the material service, and from those other internal services which, even if not directly connected to the material services, are nonetheless significant to the functioning of the firm and therefore its ability to provide the material service. A failure in one of the CTP's mapped resources could have a significant impact on its ability to deliver a material service. As a result, IIF recommends modifying section 5.2 of the draft Supervisory Statement to say (proposed new text in ***bold italicized font***), "As noted in section 3, the CTP Operational Risk and Resilience Requirements only apply to a CTP's material services, ***including the resources, assets, and technology, material to the delivery, support and maintenance of each material service it provides***." IIF's suggested modification would explicitly require CTPs to consider resilience of their resources against the operational resilience requirements.

While IIF members broadly support the UK Authorities' general approach, we have identified some areas in the consultation where further refinement may strengthen the proposals, or which would benefit from greater clarity. These recommendations are included in more detail below.

(ii) International Coordination

IIF members strongly support international co-ordination in relation to CTP requirements and oversight, and therefore welcome the UK Authorities' desire to design an interoperable regulatory regime. This is very important to avoid regulatory fragmentation given the cross-border nature of many CTPs' business models, and for FIs/FMIs that operate in multiple jurisdictions. Given that other jurisdictions are developing their own approaches to CTP oversight and resilience requirements, such as DORA in the European Union (EU), it is important for the UK Authorities to continue to "strengthen cooperation in the area of CTPs with the regulators responsible for these regimes through existing or, if necessary, new cooperation arrangements" as stated in the consultation. Specifically, the UK Authorities could consider whether a formal approach to recognition of equivalent third-country regulatory regimes for CTP resilience could be developed.

(iii) Designation of CTPs

IIF members support authorities, such as UK HMT, designating third parties as critical given that individual FIs/FMIs do not have sufficient information on which, and in what capacity, providers are being used across the industry. IIF members further support the UK Authorities should make recommendations to HMT on these designations based on their analysis of relevant data and information. As per the consultation, IIF members agree that the materiality of a third party's services and concentration in the provision of third-party services to FIs and FMIs should be the main factors for designating CTPs, with the other relevant factors being considered in the context of a material service or concentration.

The IIF notes that Section 2.20 of the consultation discusses including substitutability as a relevant factor to take into account when identifying potential CTPs. IIF members advise the UK Authorities against considering substitutability of a third party's services to FIs/FMIs as a relevant factor on its own. While there are some services where substitutability may be achieved, these are often limited to services where the components of the services are largely standard (e.g., trade matching). However, for more complex services such as cloud services, perceived substitutability may not be feasible. As noted in the U.S. Treasury's 2023 Report on the financial

services sector's adoption of cloud services,[8] few firms have considered using a multi-vendor approach for more complex services like IaaS which would be needed for achieving substitutability. There were several reasons cited in the report including technical challenges such as *"the need for staff with development expertise in multiple cloud environments, as well as accompanying cloud security and risk management expertise."*[9] As few FIs/FMIs can achieve substitutability of some large third parties at this time, a standalone substitutability factor/criterion may be easily triggered, rendering it ineffective and leading to an inflated number of designated CTPs. However, substitutability may be a relevant *secondary consideration* when analyzing whether to identify a third-party provider as critical. In some instances, substitutability may exist which could mitigate the concerns about criticality of a third-party provider; in other instances, lack of substitutable options for a third-party that is providing material services could reinforce the designation of that third party as critical.

In terms of the data that the UK Authorities will use for their analysis of CTPs and the future development of an outsourcing and third-party (OATP) register, IIF members would note that data from FIs and FMIs alone may not be sufficient to provide the UK Authorities with a full understanding of the interconnectedness between third party providers and the UK financial system. The UK Authorities may need to gather supply chain information directly from CTPs. For example, FI/FMIs may directly utilize the same third-party services as a CTP and, as an outcome, may result in a FI/FMI fourth-party service concentration.[10] Similarly, if several CTPs use the same third-party service provider in the provision of material services to FIs/FMIs, even if the third-party provider is not used directly by many FIs/FMIs, there could be a widespread impact in the financial system of disruption at the third-party provider in the event of an operational incident.

(iv) Information sharing

IIF members support UK Authorities requiring CTPs to share certain information with FI/FMIs as the designated information may assist FIs/FMIs in delivering on their own operational resilience targets and commitments, as part of their existing third-party risk management and due diligence activities, and/or may provide for more comprehensive operational resilience testing. Outlining a method for CTPs to provide information in a comparable, consistent, and structured manner may assist the UK Authorities, FIs/FMIs and CTPs themselves with understanding and identifying operational resilience gaps and developing more comprehensive approaches for addressing operational resilience within the sector.

However, as recognized in the consultation paper, there are important legal, privacy and security considerations around data requirements, sharing (including cross-border), use and storage. It is important that provision is made for cases in which a CTP sharing information about specific incidents could indicate or reveal resilience vulnerabilities at particular FIs/FMIs, or indeed the CTP itself. The consultation paper does not currently explicitly discuss the specific arrangements for cross-border data sharing between CTPs and regulatory authorities or FIs/FMIs, and how they could ensure an appropriate level of protection for confidential information concerning individual FIs/FMIs or CTPs. Part of the background, of course, are adjacent issues such as data localization

[8] US Treasury (2023), "The Financial Services Sector's Adoption of Cloud Services".
[9] Ibid, p. 26.
[10] This is recognized in proposed Requirement 3, which proposes that a CTP would have to *"be transparent with the regulators and its FI and FMI customers about which parts of its supply chain are essential to its delivery of material services."*

(i.e., rules that require data to be stored and processed locally), or other data barriers which can impede cross-border data flows.[11]

Consistent with IIF comments in past consultations on this topic, IIF members request that the UK Authorities consider how supervisory authorities will store and protect information gathered about and from CTPs. The collection of information described in this Proposal would lead to the UK Authorities being a centralized recipient of information about important business services in the financial sector both from FIs/FMIs and, in future, from CTPs too. Therefore, it is critically important that such information and data are stored and protected in an extremely secure manner to protect the security of FIs/FMIs, CTPs and, ultimately, real economy customers.

(v) Impacts on FIs/FMIs

As also stated in the consultation, although the specific proposals are primarily for CTPs, they will have important impacts on FIs/FMIs as clients of CTPs. FIs/FMIs are expected to benefit from the assumed reduction of systemic risk to the wider financial system as a result of heightened supervisory expectations and, ultimately, greater operational resilience of CTPs. As a general matter, IIF members welcome the ability to have greater collaboration on achieving stronger resilience across the wider financial system. However, new requirements for CTPs to map the provision of certain material business services, undertake enhanced testing, etc. will require them to demand more information from their FI/FMI customers (further discussed below). There could also be potential unintended consequences of the regime, such as a fall in the number of third parties willing to provide certain services at a given price, for example if the revenue earned from a service does not sufficiently offset the increased compliance costs. In such a scenario, reduced or more expensive access to third-party services may limit FI/FMI access to innovative technological solutions.

IIF members note that the PRA has utilized register information in the past to identify FI/FMIs that may have been impacted by a disruption to a third-party provider. The CTP regime would introduce incident reporting whereby a CTP's clients could be listed alongside a potential disruption[12], and it is likely that UK Authorities and supervisors could request further information from FIs/FMIs concerning any incident. FI/FMIs will use CTP material services in different ways and may 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 FI's/FMI's important business services. Supervisory requests for information can elicit an extensive effort from the recipient firm and create follow-up activity between the three lines of defense, which may be disproportionate to the firm's actual operational risk assessment. We therefore recommend that the UK Authorities exercise discretion when requesting further information from FIs/FMIs directly about an incident at a CTP, so as to avoid generating significant additional work for firms' incident response teams or unintended signalling about the materiality of an incident to the firm in question.

An important implication of the proposed CTPs requirements relates to information gathering by CTPs from their FI/FMI customers. IIF members question how much additional information they

[11] Further discussed in IIF 2021.

[12] Section 7.15 of the draft Supervisory Statement: *"a CTP's initial incident notification to the regulators must also include the following information relating to the relevant incident's potential impact on the stability of, or confidence in the UK's financial system (likewise in so far as they are aware at the time of the submission): the names and number of firms and FMIs affected…".*

might need to provide for CTPs to be able to assess to whom they are providing material business services, and the impact tolerances being managed to in the financial sector. There is also a concern that this may be challenging for CTPs to do without access to sensitive proprietary information from FIs/FMIs or the OATP register.

Specifically in relation to proposed Requirement 7[13] on Incident Management, Response and Recovery measures, it is challenging to understand how this would be achieved and the necessary dynamics between a CTP, its FI/FMI clients, and the UK Authorities. Under one potential model, FIs/FMIs would provide information about their impact tolerances for a particular material service to a CTP and the CTP would account for these in the setting of its maximum tolerable level of disruption (MTLD). This would be challenging to achieve operationally, also given the differences across the financial sector in terms of setting impact tolerances. In another model, a CTP could share information about their MTLD with FIs/FMIs for review to ensure that their MTLDs are –or become over time– compatible to the extent possible with the impact tolerances set by FIs/FMIs for their own important business services, while recognizing that such impact tolerances vary across the sector. This may be a challenging model to operationalize given the number of existing relationships a CTP may have, and future relationships it may enter into. A third model could put the UK Authorities in the middle as a central node of information, guiding a CTP on FI/FMI impact tolerances across the sector. However, this would be challenging for supervisors as they may not have full insights into the different ways each FI/FMI uses a CSP's material services. Each model has advantages and challenges; it may be valuable for the UK Authorities to further consider, in consultation with large third-party providers and FIs/FMIs, the most practical approach to take to achieve the objectives of Requirement 7.

IIF members note the comments in the consultation that the proposed new requirements for CTPs will not diminish the current expectations for FIs/FMIs in relation to operational resilience and third-party risk management. FIs and FMIs recognize that, while they cannot observe or respond to certain risk concentrations across the sector and other systemic issues, they can mitigate some microprudential risks associated with CTPs through effective third-party risk management policies, processes, and controls.

The remainder of this comment letter sets out responses to specific questions posed by the UK Authorities in the Consultation Paper.

Responses to Select 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?

See comments in Section (i), above.

[13] Requirement 7, section 5.40 of the draft Supervisory Statement: "These metrics and targets should: take into account and (to the extent possible) be compatible with the impact tolerances that firms and FMIs have set for any important business services that are supported by the material service".

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?**

See comments in Section (i), above.

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'?**

No specific comments.

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?**

See comments in Section (i), above.

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?**

Requirement 1: Governance

This requirement states that every CTP should appoint an "appropriately-qualified employee" to act as a central point of contact for regulators at a CTP. Some third-party providers that have significant links to the financial services sector are large and offer hundreds of services. It may not be practical for one individual to be a point of contact on all topics. In this area, the UK Authorities could consider a more principles-based approach which requires that there is ***at least one*** appropriately-qualified employee point of contact for the regulators, without specifying a specific number of employees. The final rule could also further expand on the meaning of "appropriately qualified", for example, whether the requirements are the same as or similar to the PRA/FCA Senior Management Functions (SMF) Regime.

Given the significance of this role, the final requirement could also require the colleague(s) to be ***"appropriately senior"*** or ***"appropriately empowered"***, as well as appropriately qualified, such that they can take the necessary decisions.

Requirement 4: Technology and Cyber Resilience

Refer to comments in Section (v), above.

We recommend that the UK Authorities make the proposed changes below (in ***bold, italicized font***) to assist CTPs with interpreting this provision. To further assist, the UK Authorities could consider providing a non-exhaustive list of examples of relationships that CTPs could consider recognizing that, as a practical and legal matter, each CTP remains obligated to identify and manage its own specific universe of subcontracting relationships and is also best placed to identify its internal technology dependencies.

> "5.18[14] The UK Authorities propose to require a CTP must ensure the resilience of any technology that delivers, maintains or ***materially*** supports ***the delivery of*** a material service, including by having:

[14] Referring to draft Supervisory Statement.

- Technology and cyber risk management and operational resilience measures
- Regular testing of those measures
- Processes and measures that reflect lessons learned from testing; and
- Processes and procedures that convey relevant and timely information to assist risk management and decision-making processes."

Requirement 7: Incident Management

Refer to comments in Section (v), above.

Requirement 8: Termination of Services

IIF members support the proposed requirement for CTPs in relation to Termination of Services. From an FI/FMI perspective, it is important to clearly differentiate and delineate between what is typically covered under Business Continuity / Disaster Recovery (BC/DR) plans and what is covered by exit strategies since these are often distinct in most firms.

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

As further discussed under 'Information Sharing' (Section (iv)), above, we would recommend that the UK Authorities elaborate on the important legal, privacy and security considerations around data requirements, sharing (including cross-border), use and storage.

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?

See comments in Section (i), above.

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?

The IIF welcomes the expectation that a CTP coordinate its crisis communications with those FIs/FMIs to which it provides material services. IIF urges the UK Authorities to consider revising section 5.45 to explicitly note that the CTP's playbook will need to include direct outreach mechanisms for FIs/FMIs known to be critically impacted by an incident. The relationship between the CTP and FIs/FMIs will be different (in terms of business relationship, contracts, and potential impact from a material operational incident) and therefore sector-level information exchange will not be sufficient for an FI/FMI that is critically impacted. By way of example, in the 2023 ION incident, there was a wide variance of impact between different ION client firms, with some ION clients experiencing material disruption while there was limited impact for others.

Accordingly, to clarify incident notification and management requirements between the CTP and FIs/FMIs, IIF recommends revising section 5.45 to include a clear requirement for a CTP to ***"communicate directly about the incident with those FIs/FMIs it knows to be, or is subsequently informed are, critically impacted by the incident, including about the cadence for incident updates,"*** in addition to the items already listed. As described below, a CTP may not know how significantly impacted all of its FI/FMI clients are *ex ante* but should respond to feedback from its critically impacted clients.

In addition, IIF members ask that the UK authorities make conservative use of CTP incident reports. We recognise that the UK authorities plan to utilise third-party registers to identify Fis/FMIs that may be exposed to an incident at a common CTP. However, as per our comments in Section (v) above, the actual impact on FIs/FMIs of an incident at a CTP can vary significantly between firms depending on the use of the service, their role in the market and the CTP's interpretation of the incident reporting scope. FIs/FMIs, in addition, have existing risk management, controls, and mitigation policies in place for their services such that incidents at a CTP may not result in any internal or external impact to a firm's services. Supervisory requests for information (RFIs) can elicit an extensive effort from the firm and create follow-up activity between the three lines of defense, which is sometimes disproportionate to the firm's actual operational risk assessment. We therefore recommend that authorities exercise discretion when requesting further information from FIs/FMIs directly about an incident at a CTP, so as to avoid generating significant additional work for firms' incident response teams or unintended signalling about the materiality of an incident to the firm in question.

Connected to this, section 7.15 of the draft Supervisory Statement requires the CTP to provide the authorities with information regarding the FIs and FMIs impacted, and details on the nature of that impact. We believe that it may often be difficult for the CTPs to provide the names of specific FI/FMIs that are impacted or the details of the potential impact at an early stage in any incident. FIs/FMIs have different resilience plans which may provide continuity of services in the event of an outage at a critical third party. As such, a CTP may be in a position simply to provide a list of all its FI/FMI clients as those which could potentially be impacted, particularly until the contours of any particular incident become clearer. However, if supervisors act on this information alone it is likely to lead to a significant amount of additional work for incident responders within FIs/FMIs, in line with our comments above. While IIF members recognize the UK Authorities may wish to make use of this information, we recommend that clear guidelines are developed, and a high threshold is applied, before RFIs are circulated to FIs/FMIs. This is especially the case if incident reporting requirements evolve to require significantly more information from firms, thus exacerbating the potential operational impacts of such reporting on firms. Any details of the impact would, due to the variance of FI/FMI CTP usage, need to be provided by the FI/FMI itself which can be done through existing reporting requirements.

Finally, we are concerned that some of the requirements in section 7.18 of the draft Supervisory Statement may create additional security risk. The use of the term "vulnerability" is unclear in this context, specifically whether it refers to a cybersecurity vulnerability or a vulnerability as the term is used in the context of the UK's operational resilience supervision. If the former, IIF members advise that vulnerabilities should not be disclosed before suitable patches are determined and released using established channels. Requiring disclosure before that time creates additional risk of widespread exploitation of the cyber vulnerability. It is also the case that certain jurisdictions may attempt to require that such information be reported for the purposes of building their own databases of vulnerabilities. We would therefore request that UK Authorities provide certainty and clarity on how "vulnerability" should be interpreted in this context given the concern noted, and potentially use an alternative term (such as ***"resilience vulnerability"*** if that would clearly describe the intended meaning).

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

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

to firms. We recommend that the definition in the draft Supervisory Statement be changed as follows (revised text in ***bold, italicized font***):

- "7.4: The incident notification requirements apply to a 'relevant incident', which is defined as either a single event or a series of linked events that actually or ***is highly likely*** ~~***has the potential***~~ **to**: seriously disrupt the delivery of a material service; or …"

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

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?

IIF members support the three phases of incident notification. The intermediate phase is very important to FIs and FMIs who require information about the progress and steps to resolve an incident to inform their own strategic and operational response.

Regarding the "Final Incident Notification" requirement (section 7.24 of the draft Supervisory Statement), we ask that the final text provides clarity that a notification will be provided by the CTP to the regulators and the FIs and FMIs ***without undue delay*** once the incident has been resolved. This notification will allow these affected parties to take appropriate actions to restore their own internal services, which is a time critical activity.

Further, root causes and lessons learned should be provided to the regulators, as well as the FIs/FMIs impacted by the incident, at an appropriate timeframe after the final incident notification. The current text conflates these two distinct steps. IIF members recommend that the UK Authorities separate the final incident notification alerting stakeholders that a service has been restored from any final analysis (e.g., root cause analysis) that must be conducted by the CTP.

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?

No specific comments.

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

The current proposals would allow a CTP to "use a range of formats for their notifications as long as they include the information specified in the regulators' draft rules and draft Supervisory Statement". In future, IIF members would encourage the UK Authorities to review the proposals developed by the Financial Stability Board (FSB) concerning the Format for Incident Reporting Exchange (FIRE) and consider their adoption when finalized to encourage greater convergence of incident reporting requirements across jurisdictions and reduce the current fragmented and duplicative requirements faced by FIs/FMIs.

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

IIF members would like more information about the proposed self-assessment requirement in terms of detail, format, and governance. It is not clear in the current consultation or draft Supervisory Statement whether or how CTPs' self-assessments would be reviewed or assured.

The IIF welcomes the requirements for the CTP to test its playbook annually and for FIs/FMIs to be included in that testing. IIF members support CTPs having the ability to determine how an appropriately representative sample is determined and to have this method reviewed and agreed to by the UK Authorities given the varying CTPs and associated services that may be in scope and the need to ensure systemically important firms are considered. Similarly, requirements related to testing methodology, whether testing the incident management playbook, table-top testing or other testing methods, should remain outcomes-focused and avoid becoming overly prescriptive or granular as they may be challenging for each unique CTP to meet.

While CTP testing should be appropriately designed and targeted, we believe that section 6.27 of the draft Supervisory Statement should be expanded to ensure that testing requirements also scope in testing of the resources including the assets and technology used to deliver, support, and maintain each material service a CTP provides if these are critical to the functioning of the CTP's material services. In order to emphasize the importance of such resources, we recommend that the requirements in section 6.13 of the draft Supervisory Statement should be expanded to include a further bullet point on ***"the assets and technology that deliver, support, and maintain that essential service."*** The description of scenario testing in section 6.9 should additionally include a reference to resources that are critical to the delivery of the material service.

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

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

In principle, IIF members can see benefits of certain additional mandatory testing for CTPs which is, for example, similar to the testing requirements for operational resilience of FIs/FMIs.

In addition to CTP-specific testing, additional testing conducted at the level of the financial sector including CTPs could support preparedness and identify interconnections and potential market dependencies. These exercises could be patterned after, and conceptually similar to, the supervisory stress tests of central counterparties. Exercises led by the relevant sectoral standard setting bodies could help to identify potential risks and help all market participants to better understand the actions they might need to take in response to those risks.

However, it would be necessary for the UK Authorities to further specify and consult on the nature of additional mandatory testing for CTPs for clarity over what it would entail.

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

The proposed Supervisory Statement includes in section 6.35 a requirement for CTPs to provide information (which is specified in 6.36 as, broadly, the results of testing and summary of the CTP's self-assessment) to FIs/ FMI on a timely basis. For the sake of clarity, it may be helpful to include explicit reference in this section to the provision of information on a timely basis and *at least annually*.

To support FIs'/FMIs' interpretation of the results of scenario testing, it would be helpful for the regulators to include a requirement for CTPs to provide information to FIs/FMIs on the scenario which was tested against.

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

See comments in Section (v), above.

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?

See comments in Section (iv), above.

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?

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

(Response to Q18 & Q19) IIF members recognize the risks discussed in the consultation of CTPs using designation as a regulatory 'kite-mark' of approval. We therefore fully support the proposal to prevent CTPs from using designation in this way and think that the comments in the consultation on misleading use of designation status provide clarity on what the designation means and how it can be used.

Nevertheless, in reality the designation of a supplier as a CTP could still shift market sentiment towards CTP vendors over those that do not carry the CTP designation even though supervisors are not recommending or endorsing any particular vendor. Designated CTPs will be required to provide FIs/FMIs with a greater level of visibility into the CTP's operational resilience capabilities. Further, designated CTPs will be held to a higher and known operational resilience standard similar in scope to the standards currently in place at FIs/FMIs. Lastly, FIs/FMIs will participate in joint exercises with designated CTPs, giving a valuable feedback loop which would support the CTP's operational resilience preparedness. Therefore, while this is the desired result of the proposed policies, there could be an unintended consequence that the ability of FIs/FMIs to engage with a third party designated as critical at this more granular level may create an environment in which FIs/FMIs are more likely to select these third parties as they are bound, by regulatory requirements, to increase their engagement. In parallel, third parties designated as CTPs would also face higher costs in terms of regulatory compliance, etc. IIF members request that the UK Authorities may want to consider potential approaches that would reduce barriers to

competition or growth by smaller, non-critical third parties and avoid exacerbating issues around market concentration.

20. Do you have any comments on the cost-benefit analysis? Do you have any comments on the regulators' proposals to restrict CTPs from indicating for marketing purposes that designation implies regulatory endorsement or that its services are superior? Are there any other measures which the regulators could consider to mitigate potential, unintended adverse impacts on competition among third party service providers as a result of the designation of CTPs?

No specific comments.

Thank you in advance for your consideration of these comments. On behalf of the IIF membership, we hope that these global industry perspectives will contribute constructively to your efforts. We would be very happy to discuss any of our comments further or to assist in any way, including providing perspectives on approaches taken in other jurisdictions. We invite you to contact Katie Rismanchi (krismanchi@iif.com), Martin Boer (mboer@iif.com), Laurence White (lwhite-advisor@iif.com) or Gloria Sanchez Soriano (gsanchezsoriano@iif.com) should you have questions or comments.

Yours Sincerely,

Katie Rismanchi
Deputy Director
Regulatory Affairs
Institute of International Finance (IIF)