FIA.org

FIA Response to RTS on subcontracting ICT services

PRELIMINARY COMMENTS

As an initial matter, FIA[1] and FIA EPTA[2] ('The Associations') appreciate the opportunity to provide feedback on this draft Regulatory Technical Standards (RTS). The Associations note that there are a few high-level comments and observations, that apply to many of the questions asked by the European Supervisory Authorities (ESAs) in the draft RTS, that we believe would be more efficient to detail at the outset of our reply. We also note these comments within the answers to each specific question where they apply.

Timing and Cost Benefit

The Associations note the significant implementation challenges and resourcing required for firms to implement extensive processes for existing arrangements as well as for new arrangements. Related to this, as the Associations note in the conclusion to this response letter, given the timing of when this RTS will be finalized relative to the effective date of DORA, the Associations also respectfully encourage the ESAs consider issuing much-needed flexibility (similar to those the ESAs have issued previously in other contexts[3], see also our conclusion section) to enable market participants sufficient time to comply with the final rules.

The cost benefit analysis seems to critically underestimate the impact of these RTS and the costs associated with their implementation and ongoing operation. In particular, the RTS states that it has "a low impact with cost of monitoring only". The Associations note that the cost benefit analysis thereby does not take into account, in particular, the significant effort needed for implementation of these requirements, the enhanced contractual negotiating required, and the costs associated with initial and ongoing data collection required from third-parties, particularly in the timeframes specified. It also overlooks the potential impact on third-party providers (TPPs) and sub-contractors and, potentially, their willingness to serve the European market. In light of the extensive requirements noted in the RTS, the Associations strongly urge the ESAs to conduct a more detailed assessment of the impact of the requirements of this RTS.

Proportionality:

The DORA legislative text establishes the application of proportionate principles to ICT third-party risk management and specifies, amongst other matters, consideration of the risks arising from contractual arrangements and the potential impact on the continuity and availability of the contracted service. Despite this intention, the RTS fails to adequately apply a proportionate and risk-based approach and sets expansive

[1] FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in Brussels, London, Singapore and Washington, D.C. Our membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from about 50 countries as well as technology vendors, law firms and other professional service providers. Our mission: To support open, transparent, and competitive markets, protect and enhance the integrity of the financial system, and promote high standards of professional conduct.

[2] FIA European Principal Traders Association (FIA EPTA) represents Europe's leading Principal Trading Firms. Our 24 members are independent market makers and providers of liquidity and risk transfer for exchanges and end-investors across Europe. We work constructively with policymakers, regulators and other market stakeholders to ensure efficient, resilient, high-quality financial markets.

[3] ESAs modification of Art 3(2) in JC 2023 84 - Final report on draft RTS to specify the policy on ICT services supporting critical or important functions)

and exhaustive risk management and contractual requirements across the *entire* subcontracting chain. Without the explicit application of a materiality threshold, the RTS risks capturing an unworkably broad supply chain scope that would not necessarily add value to risk management. In fact, it would reduce a financial entities' ability to effectively manage relationships that pose the most risk to them from an ICT risk perspective as it will require financial entities to divert resources to managing subcontractors that would not pose a material resilience impact.

We wish to emphasize that (i) not all ICT services supporting critical or important functions carry the same level of risk (or importance) to a financial entity; and (ii) not all sub-contractors supporting any aspect of critical or important functions, or a material part thereof, are of equal risk to the financial entity regardless of the sub-contractor's role, or potential impact on the financial entity or its delivery of services. The Associations would encourage the ESAs to revise the RTS to more fully reflect the proportionality provisions within DORA's legislative text and, in particular, Articles 28(2) and Article 30(5). The application of a materiality threshold in accordance with a proportionate and risk-based approach will ensure that financial entities are able to identify and monitor the material risks along the subcontracting chain, and those subcontractors whose disruption or failure could lead to a material impact to service provision. This approach would also reflect the intention in the DORA legislative text for a proportionate approach to ICT third-party risk management.

This could be achieved, at a minimum, by **aligning the scope of subcontractors captured in the final draft of the implementing technical standard on the Register with this RTS**. In the Register ITS, '*material subcontractors*' is appropriately defined as "*only those subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof, including all the subcontractors providing ICT services whose disruption would impair the security or the continuity of the service provision*". This reflects a proportionate and risk-based supply chain scope that should be aligned to a financial entities' due diligence, oversight and reporting practices (i.e. across both the register and risk management framework). The Associations would strongly recommend for the definition of material subcontractors to be reflected in the final draft of the subcontracting RTS. This alignment would be essential for the consistent approach to and application of the Level 1 and Level 2 third-party risk management requirements.

Furthermore, applying both materiality and proportionality would in no way undermine the requirements of Article 29(2) of DORA, relating to a firm's ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.

For the purpose of this response, all references to 'subcontractors' should be understood to encompass "only those subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof", i.e. material subcontractors.

International regulatory approach

In order to ensure the application of an appropriate risk-based approach, we wish to highlight existing international standards related to the management of sub-contracting risks and, in particular, the FSB's toolkit for enhancing third-party risk management and oversight (FSB Toolkit). The FSB recognizes the need to apply the principle of proportionality in the management of risks from "*key nth party service providers*". This would allow financial entities to focus on those subcontractors that are knowingly essential to the delivery of critical

services to financial institutions or which have access to confidential or sensitive data belonging to the financial institution. The FSB Toolkit notes in Section 3.5.1 that, particularly in areas such as ICT, there are challenges and practical limitations to a financial entity's ability to directly assess and manage every unique risk across each element of their third-party service provider supply chains. Hence, the FSB recognises the need to apply the principle of proportionality in the management of supply chain risks. We strongly urge the ESAs to have regard to the commentary by the FSB on the management of supply chain risks.

We also note that the FSB approach is to provide a toolkit i.e. considerations for financial entities to take into account when managing third party risks. Given the wide array of financial entities subject to DORA, the Associations propose that an RTS that incorporates "considerations" instead of some prescriptive requirements may ultimately prove more fit for purpose in guiding and ensuring different financial entities effectively oversee their ICT risk.

Scope

The Associations note the point made by the ESAs in 3(6) of the Background and Rationale section of the draft RTS that ICT intragroup subcontractors should be considered as ICT TPPs. The comments in this letter apply equally to the impact of the RTS on ICT intragroup subcontractors as they do to external ICT TPPs although we appreciate that the challenges raised are more pronounced for the management of subcontractors linked to external third parties. Proportionality, materiality, and contractual separateness are all equally relevant in a group context.

Question 1: Are Articles 1 and 2 sufficiently clear?

As noted above in the proportionality comments, it is critical that subcontractors are limited to material subcontractors.

Certain risk elements in **Article 1** are not relevant for assessing the level of risk associated with the use of subcontractors, or with material changes to subcontracting arrangements. The factors in subparagraphs 1(f) – 1(h) are not impacted by the use of the subcontractor. Rather, these considerations are linked to the inherent risk level of the financial entity's planned usage of the service provided by the third party provider (TPP). We therefore recommend that these elements are removed. We note that these are already captured as part of the risk considerations set out in Article 1 of the RTS specifying the policy on ICT services supporting critical or important functions.

Question 2: Is Article 3 appropriate and sufficiently clear?

Whilst FIA agrees with the need for financial entities to manage the risks associated with the use of sub-contractors, the regulatory focus should be on ensuring that financial entities implement robust risk management frameworks underpinned by comprehensive, risk-based due diligence processes, contractual frameworks that provide for flow down of risk management obligations to material subcontractors and risk-informed oversight measures that are commensurate to the level of risk and complexity of the third-party engagement.

The more explicit requirement in **Article 3(1)(c)** to ensure that certain clauses of the contract between the financial entity and ICT TPP are replicated in the contract between the ICT TPP and its subcontractor risks undermining fundamental contractual legal principles aimed at preserving confidentiality between contracting parties. As such, making a financial entity's compliance with its own obligations contingent upon its ability to have visibility and a say in contract formation as a non-party is inherently problematic. This requirement goes well beyond Article 30 that does not prescribe the conditions that the financial entity shall indicate when authorising the use of sub-contractors. **The focus should be on ensuring the contractual framework between a financial entity and an ICT TPP provides for the flow down of contractual obligations.** This would reach the same intended outcome, whilst remaining achievable and within established legal boundaries.

Moreover, this could also leave financial entities with limited options for meeting this requirement if an ICT provider is not prepared to share this information with the financial entity. The financial entity would be required to terminate the contract for ICT that supports a critical or important function, regardless of whether there were other providers in the market willing to provide the financial entity with the level of information required in the RTS.

Article 3(1)(e) introduces the expectation for financial entities to monitor and oversee subcontractors *directly* where possible and appropriate. FIA members expect to rely on existing comprehensive, risk-based due diligence processes and supplier controls for ongoing due diligence activities to ensure that supply chain risks are managed and mitigated. It is important to note that this does not equate to the delegation of a financial entity's responsibility to manage subcontractor risk along the supply chain, but rather it is fundamental to strategic and effective risk mitigation practices that financial entities leverage a third-party's (i) direct contractual relationship with its subcontractors which can enforce the flow down of risk management measures and supplier controls and (ii) expertise and nuanced understanding of their service and control environments.

A financial entity's third-party risk management program is the most effective way of ensuring the risk management measures relating to subcontractors are upheld, and are enforceable, through the contractual framework between the financial entity and its third party which frequently include the following provisions:

- third-parties must seek approval or consent before engaging a 'material' subcontractor. A materiality threshold is applied to this requirement so that financial entities and third-parties can focus on managing only those subcontractors which present a risk to the delivery of the service;
- third-parties are required to do due diligence on their subcontractors and to make the results of this due diligence available to the financial entity upon request. This obligation typically applies to any subcontractor, regardless of tier, that is 'material' to the delivery of the service. The ability to access due diligence materials is an important tool for providing visibility into a financial entity's risk posture (as it feeds into the risk assessment) and contractual flow down;

- third parties are contractually obligated to flow down their risk management and oversight obligations to the entire supply chain;
- third parties are required to stand behind the performance of their subcontractors;
- financial entities assess a third-parties' control environments initially at onboarding and periodically on an ongoing basis, at a frequency and rigor that is reflective of the inherent risk of the third-party engagement. Any deficiencies identified in the third-parties' oversight of its subcontractors are documented and appropriate action is taken.

We would therefore advocate for a balanced and outcomes-based approach that allows financial entities to effectively manage material supply chain risks, leverage contractual frameworks and third-party expertise, whilst remaining ultimately accountable to assess and monitor the risks associated with the ICT subcontracting chain, and their compliance with their own legislative and regulatory obligations.

Regarding **Article 3(h)**, while the Associations recognizes the importance of considering concentration risks, from the individual entity perspective, a financial entity would generally take into consideration the potential impact of its use of a third-party service provider across multiple services and review concentration risks as part of ongoing monitoring of service providers. Financial entities, however, also need to take a balanced approach and weigh any risk of service provider concentration against any gains in resiliency, efficiency, or effectiveness of using a third-party to deliver services to its members or clients. To this point, the Associations emphasize that any requirements to consider concentration risks should enable the financial entity to take a balanced, risk-based approach.

Additional comments:
Regarding section 1f, we believe it is very challenging for a financial entity to assess the direct impact of the failure of a sub-contractor (particularly level 2 or 3 or beyond) on the overall delivery of an ICT service supporting a critical or important function.

We note it is implicit in the draft RTS that 1) financial entities will have significant negotiating power vis a vis ICT TPPs and 2) that direct ICT TPPs to financial services entities in the EU and their subcontractors will adapt to these requirements if they wish to continue to provide ICT services to regulated firms. While this may be the case for the largest of EU financial firms and the ICT TPPs that focus on supporting the largest EU financial firms, DORA applies to a very wide number of financial entities, including smaller firms. Financial entities in scope for DORA may also use niche or bespoke providers specific to their sector or strategic approach and may leverage specialist ICT providers outsider the European Union. The range of financial entities, the range of their potential service providers and the relative heterogeneity of their needs and negotiating power needs to be taken into consideration in this RTS.

Moreover, third-party providers may not have any financial or commercial incentive to meet the regulatory requirements being imposed on smaller entities under the RTS. An unintended consequence therefore of the RTS is that it may in fact increase concentration risk as financial entities are forced to use only larger third-

party ICT providers that are willing and capable of meeting the requirements of EU regulated financial entities, while many more diverse and equally robust providers may choose to exit the EU market for their services.

Question 3: Is Article 4 appropriate and sufficiently clear?

The RTS applies risk management and contracting requirements to the *entire* ICT subcontracting chain of an ICT third party provider in respect of services supporting critical or important functions, or material parts thereof. The RTS should only capture ICT services supporting a material part of critical functions to prevent the application of onerous requirements to some minor services supporting a critical function. The Associations recommend that the ESAs limit the scope of the subcontractors to be in scope for the RTS to only those that are knowingly essential to the delivery of a critical or important function. We note that this approach would be consistent with the ESAs adding a further element of proportionality in the Final Report on Register of Information RTS to focus on only those subcontractors supporting a material part of a critical or important function.

As set out in more detail earlier in this letter, the Associations are concerned that Article 4 as drafted does not sufficiently allow for the application of either proportionality or materiality and therefore risks capturing an unworkably broad scope of subcontractors. Furthermore, for reasons stated above and in the proportionality section of this response, Article 4c should also be limited to relevant risks.

While Article 4(i) is seemingly sound, the risk is that financial entities would be expected to exercise those audit rights to the same level as with third-party service providers. This could lead to a significant increase in compliance activities for financial entities, third-parties and subcontractors, with minimal indication that risk would be managed more effectively. Financial entities would need to conduct several additional audits across the subcontractor base rather than on one entity - the third-party. This will multiply the number of resources financial entities, third-parties and subcontractors will need to manage for compliance activities and divert valuable resources from managing the most relevant risks.

Question 4: Is Article 5 appropriate and sufficiently clear?

The Associations are of the view that this article is not sufficiently clear, and is potentially overly broad as drafted.

Article 5(1) as drafted states that the financial entity shall fully monitor the ICT subcontracting chain, and then notes that the documentation related thereto can be based on the ICT register firms must maintain and can be based on information provided by the ICT TPP. As noted elsewhere, this does not seem to include any element of materiality, which would be helpful in this context as well. In addition, if the expectation is that financial entities may discharge their monitoring obligations through reporting to them by the ICT TPP, as would be customary, the RTS would benefit from being clarified that this is an acceptable manner of monitoring contracting.

With regard to 5(2), a financial entity's ability to access an ICT TPP's own contracts with subcontractors is likely not to be appropriate or commercially feasible due to commercial and confidentiality constraints. As such,

the expectation for the financial entity to monitor subcontracting chain through the review of contractual documentation between the ICT TPP and its subcontractor introduces significant legal, commercial and operational complexity.

It also raises the possibility of an impact to the core common law legal doctrine of contractual privity, by giving an entity which is not a party to the contract between ICT service provider and its subcontractor visibility over and a say in contract formation. This would also risk undermining the third-party's ability to negotiate suitable terms with its subcontractors.

As noted above, the contractual framework between the financial entity and third-party should provide for the cascading of obligations along the supply chain in respect of material subcontractors, including that these be specified or reflected in downstream contractual arrangements. Requiring financial entities to review contractual documentation should therefore not be a necessary measure. The regulatory emphasis should therefore be on robust contractual frameworks focusing on outcomes-based measures that ensure effective risk management and regulatory compliance, thereby allowing contracting parties the flexibility to negotiate and agree contractual terms that reflect the specific circumstances and risks of the third-party and/or subcontractor engagement.

This requirement would have a significant real-world impact if it were to be operationalised – particularly if the expectation extended along the entire subcontracting chain. The sheer volume of thousands of financial services firms intervening in contractual negotiations would impose a huge administrative burden, extend negotiation timelines and potential industry-wide disruption that itself would risk the stability of the financial system.

Finally, we would like to remind the ESAs that a financial entity should have the freedom to use any relevant available information (such as certificates of compliance and third party certifications) in order to reach the required level of assurances in line with Article 6(3) of the RTS to specify the policy on ICT services supporting critical or important functions provided by ICT TPPs. This would prevent duplicative efforts on the part of financial entities and third-party service providers and standardizes the information required. Large third-party vendors already publish such independent certifications and certificates of compliance.

Question 5: Is Article 6 and 7 appropriate and sufficiently clear?

Whilst financial entities should have a right to be advised of material changes to the sub-contracting chain, we do not think it is realistic to expect that financial entities will be able to enforce a right of veto in the appointment of a new sub-contractor in all but exceptional cases.

Article 6(2): The requirement to provide risk assessment results to the third-party in respect of any notified material changes will create an administrative burden without proportionate benefits to risk management.

Articles 6(3) and (4): The requirement that financial entities have the right to approve or modify changes to subcontracting arrangements may be incompatible with the one-to-many nature of public cloud services and other technology providers, which service multiple financial entities from a single infrastructure. In introducing this model, the real-world impact of a service provider having to await and manage approval or

non-objections from numerous financial entities would not only create a substantial administrative burden, but could lead to the loss of access to key services, negatively impacting resilience and competitive capabilities. We therefore suggest this paragraph is removed, and have proposed amendments to paragraph (4) which appropriately captures the notification process while reflecting the practical limitations of such models.

1) *In case of any material changes to subcontracting arrangements, the financial entity shall ensure, through the ICT contractual arrangement with its ICT third-party service provider, that it is informed with a sufficient advance notice period to assess the impact on the risks it is or might be exposed to, in particular where such changes might affect the ability of the ICT third-party service provider to meet its obligations under the contractual agreement, and with regard to changes considering the elements listed in Article 1.*

2) *The financial entity shall inform the ICT third-party service provider of* ***any objections to the proposed changes*** ~~*its risk assessment results*~~ *as referred to in paragraph 1) by the end of the notice period.*

~~*3) The financial entity shall require that the ICT third-party service provider implements the material changes only after the financial entity has either approved or not objected to the changes by the end of the notice period.*~~

4) *The financial entity shall have a right to* ***either (a)*** *request modifications to the proposed subcontracting changes before their implementation* ***or (b) terminate the agreement*** *if the risk assessment referred to in paragraph 1) concludes that the planned subcontracting or changes to subcontracting by the ICT third-party service provider exposes the financial entity to risks as specified in Article 3(1) that exceed its risk appetite.*

Furthermore, the RTS do not recognize the impact that this requirement could have on sub-contractors themselves that may have many contractual relationships. This could be significantly burdensome and some may decide, as mentioned earlier, to restrict business or exit the market.

Timing

Article 8 – Financial entities will need time to amend contract clauses with third-parties. The final text for the subcontracting RTS is expected in July 2024, while compliance is expected by January 2025. We request that the ESAs consider a compliance date for the end of 2025 to permit time to review and amend contracts, where necessary. Repapering to comply with the requirements, if fully possible, would take a very significant amount of time. Without a deferred compliance date, many firms are unlikely to be ready by the January 2025 application date for DORA.

As an alternative, we would suggest that the ESAs adopt the same approach as in the recently published final RTS on the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554, where the ESAs provide additional flexibility to implement a high number of amended contractual arrangements in a timely

manner. In particular, instead of specific timelines, the RTS now requires the financial entity to 'document the planned timeline' (response to feedback from market participants on Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?). Given the very short implementation period (6 months) we request to provide for at least similar requirements for the period starting 17 July 2024.