FIA.org

FIA position on subcontracting of ICT services

The purpose of this communication is to reiterate industry's position on the application of proportionate principles to supply chain risk management and alignment with best practices in the context of the requirements set out in the final draft regulatory technical standards on subcontracting ICT services supporting critical or important functions (CIFs) ('Subcontracting RTS').

We appreciate efforts by the European Supervisory Authorities (ESAs) to drive a proportionate and risk-based approach to the identification and oversight of subcontractors in the ICT services supply chain. We acknowledge that, in seeking to address potential sources of risk beyond the direct supplier due to long and complex ICT services supply chains, and to better align with a risk-based approach in the Subcontracting RTS the ESAs have:

(i) indicated that financial entities must have sight of the overall ICT supply chain (i.e. through requirements that financial entities identify the overall chain of subcontractors providing ICT services supporting CIFs);

(ii) differentiated this broader expectation from a more-risk based expectation that financial entities put a particular focus on subcontractors that effectively underpin ICT services supporting CIFs (i.e. subcontractors whose disruption would impair the security or the continuity of the service provision).

We also appreciate efforts by the European Commission (Commission) to further ensure the appropriate application of proportionate principles to the ESAs approach. To that end, it is important that in further embedding a proportionate and risk-based approach to the Subcontracting RTS, regulatory expectations reflect strong, workable third-party oversight practices which address *material* risks and the legal and practical realities of supply chain risk and supplier dynamics. This includes consideration of the fundamental third-party risk management principles outlined below.

In the context of the subcontracting RTS, we strongly recommend consideration by the Commission of the following positions:

1) **The expansion of expectations to monitor or oversee the entire ICT supply chain diverts resources away from managing the real risk drivers** (i.e. subcontractors that effectively underpin ICT services supporting CIFs). We acknowledge the ESAs' objectives and intention to enhance supply chain oversight practices to ensure financial entities identify all sources of ICT risk. However, the expectation to identify the overall chain of ICT subcontractors providing ICT services supporting CIFs is inconsistent with a proportionate and risk-based approach and substantially expands the scope of certain requirements in the subcontracting RTS beyond what is necessary and feasible. We recommend that the scope of *all* requirements in the Subcontracting RTS to be limited to subcontractors that effectively underpin ICT services supporting CIFs, and this application of materiality will be reflected in the flow-down of risk-management obligations to downstream agreements with material subcontractors. In practice, this means that all references to "*subcontractors providing ICT services supporting CIFs*" in the Subcontracting RTS would be replaced by "*subcontractors effectively underpinning ICT services supporting CIFs*" (i.e. material subcontractors).

FIA.org

It is important that the obligation to monitor the full supplier chain should not come at a cost of invalidating the contractual commitments by ICT TPPs. Managing the full ICT supply chain should be based on risk-based decisions.

2) **The application of proportionate and risk-based approach to supply chain risk management must be based on materiality, and not subcontractor rank**. Recognizing that financial entities are required to manage 'material' risks along the entire supply chain, irrespective of the position or rank of the subcontractor. That said, any proposal to limit the application of supply chain risk management requirements on the basis of subcontractor rank would deviate from a true risk-based approach. Such an approach diverges from international standards, existing regulatory expectations and established third-party risk management principles. Additionally, it would put at risk established risk-management and contractual frameworks and have potentially problematic implications for how contractual arrangements with suppliers are structured and negotiated.

The above positions reflect and are consistent with the following fundamental third-party risk management principles:

- A financial entities' resources should focus on overseeing elements of the supply chain that it has determined are material – not every single participant in the chain regardless of their materiality and risk they pose to the delivery of the service provision.
- A comprehensive and risk-based approach to supply chain risk management involves identifying and assessing material subcontractors, and applying due diligence and risk-based controls to manage and mitigate any associated risks.
- The management of material subcontractor risk is upheld, and enforceable, through the contractual framework between a financial entity and its third-party which provides for the flow down of risk management and oversight obligations to the entire supply chain. This includes assessing a third-parties' control environment 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.
- Material supply chain risks may occur anywhere in the supply chain and material subcontractors are not always third or fourth parties (although this is often the case). As a result, financial entities require that third-parties identify and due diligence material subcontractors across the entire supply chain.

We acknowledge that the Commission is currently focused on finalising the adoption of remaining secondary legislation and greatly appreciate the Commission's consideration of the points outlined in this letter. We remain at the Commission's disposal to assist in resolving any remaining challenges with regard to the requirements relating to subcontracting risk-management in the Subcontracting RTS, or other areas of interest as needed.