11 September 2023

**FIA position on the ESAs first batch of DORA policy products**

**Public consultation on draft Regulatory Technical Standards to specify the detailed content of the policy in relation to 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**

FIA appreciates the opportunity to comment on the European Supervisory Authorities' (ESAs) first batch of DORA policy products. We support the ESAs aim to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. However, we would like to highlight remaining industry concerns in our responses below.

**Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?**

FIA shares remaining industry doubts and concerns regarding the application of proportionality and the level of application:

Financial Entities' (FEs) third-party risk management programs establish an overarching framework that allows oversight to be tailored to the specific risks of a third-party relationship. The RTS should serve to better inform the principled considerations set out in existing European Banking Authority (EBA)/ European Securities and Markets Authority (ESMA) guidance and extended risk-agnostic third-party policy requirements under the existing frameworks consistently with an outcomes-based approach. The RTS instead takes a far more prescriptive approach, including in requiring that certain risk management processes and practices – which are current framework requirements under the EBA Outsourcing Guidelines – are explicitly set out within a firm's ICT policy.

We encourage the ESAs to focus any new policy standards on principles and intended outcomes, rather than mandating prescriptive processes, procedures or governance which would not provide additional benefit to existing risk management.

A disparate policy covering only ICT third-party service providers should therefore not be mandated under the RTS, as this would not provide additional benefit to existing risk management and decision-making processes. FEs should be able to rely on and enhance existing policies and standards with any unique ICT-related considerations.

- Article 1 of the Delegated Regulation should recognise that there is a difference in risk profile between a third party provider and an intra-group provider. As noted within recital 31 of DORA, "*when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment*." The current wording of Article 1 could however be read to mean that intra-group providers are in fact higher risk. The following clarification is therefore recommended: "*whether the ICT service provider is a third party, as opposed to being part of the same group of the financial entity*."

- We object to the inclusion of "*the location of the ICT third-party service provider or its parent company*" within Article 1 as an increased complexity or risk. This fails to take account of the third country provisions established in relation to Critical Third Parties as part of the Level 1 DORA text, under Article 36 on the exercise of powers of the Lead Overseer outside the Union, and in any event the location of the third party is already addressed under Article 4 of the Delegated Regulation. The latter provision is preferred as a more direct replication of the existing EBA Guidelines.

**Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?**

Given DORA requires holistic management of ICT policy across the own business and supply chain, attention should be given to the extent this would pose operational challenges for financial entities in the delineation and ownership of the governance of the ICT services. We welcome further discussion around this topic.

**Question 3: Is article 4 appropriate and sufficiently clear?**

No. We believe 'subcontractors' should be removed from Article 4, as financial entities would find it difficult to obtain the relevant information.

**Question 4: Is article 5 appropriate and sufficiently clear?**

No. We would find necessary to establish a grace period for the renegotiation of legacy contracts, allowing these provisions to be implemented as contracts mature and come up for renegotiation. A remediation requirement of existing contracts would lead to a multi-year programme.

**Question 5: Are articles 6 and 7 appropriate and sufficiently clear?**

We appreciate the ESAs efforts to leverage and align the requirements relating to the risk assessment and due diligence to existing guidelines. As noted above, the goal should be to ensure an outcomes-based approach that avoids a risk-specific framework and would allow FEs to leverage existing TPRM frameworks and practices, tailoring those to the specific risks as needed. The industry seeks confirmation on whether existing risk assessments can be relied upon for the purposes of DORA.

FIA supports utilizing various methods as part of the process to select and assess prospective ICT third-party service providers. FIA cautions, however, against requiring financial entities to address each element listed in Article 7(3)(C) and instead allow financial entities to determine the most appropriate element(s) to include in their selection and assessment processes based on the financial entities' own risk management frameworks.

**Question 6: Is article 8 appropriate and sufficiently clear?**

Yes. The requirements in Article 8 align with existing guidance in the EBA Outsourcing Guidelines on the approach to and governance of intragroup arrangements, consistently with a harmonised and outcomes-based regulatory approach.

**Question 7: Is article 9 appropriate and sufficiently clear?**

Yes. The requirements in Article 9 align substantially with existing guidance in the EBA Outsourcing Guidelines. However, to reflect a truly outcomes-based regulatory approach, the requirement that contractual arrangements are 'specified' in the policy itself should be omitted. The RTS should set out the principles surrounding contractual arrangements with ICT third-party providers, without such prescriptive requirements that focus on form over substance.

**Question 8: Is article 10 appropriate and sufficiently clear?**

FIA shares below remaining industry doubts and concerns:

- Article 10(1) currently states that "*The policy [on monitoring of the contractual arrangements] should also specify measures that apply when service levels are not met including, where appropriate* ***penalties***." The use of the word penalty is not seen as appropriate in this context and should be deleted: "*the policy should also specify measures that apply when service levels are not met*."

- Article 10(1) also requires FEs to monitor ICT third party services providers' compliance with requirements regarding the confidentiality, availability, integrity and ***authenticity*** of data and information. It is unclear what is meant by "authenticity" in this context, which is a term that is generally used in the context of biometric data. We recommend this is amended to "***accuracy***" of data and information to align with existing concepts and terminology in EU data protection law and current outsourcing guidelines.

- FIA requests further clarification on how financial entities should interpret "se*curity payment related incidents*" under Article 10(2)(d).

- Article 10.2.e requires financial entities to conduct an independent review and compliance audits with legal and regulatory requirements and policies for third-party service providers supporting critical or important functions. This requirement is likely not a scalable process for third-party service providers. If each financial entity performed an independent audit with their third-party service provider, it would lead to numerous and potentially conflicting requirements from clients. FIA requests that the ESAs consider the current third-party risk management practices, such as meeting with technical subject matter experts, due diligence questionnaires and reviewing relevant audit reports, and determine if these practices meet the objective of 10.2.e.

**Question 9: Is article 11 appropriate and sufficiently clear?**

No. The requirement for exit plans on *each* ICT service to be periodically tested is impractical and not reflective of current industry practice. We recommend that the requirement for testing of each exit plan is removed.

FIA believes that as currently written, Article 11 blurs the delineation between exit plans and Business Continuity Planning / Disaster Recovery (BC/DR). BC/DR plans typically focus on short-term solutions that can be executed through the course of an operational event, like service disruptions, until the business can return to normal operations. Article 11, however, includes service interruptions as a factor to take into account in a documented exit plan. FIA requests for the ESAs to limit exit strategies to scenarios with longer transfer timeframes such as the unexpected termination of a relevant contractual arrangement (as currently mentioned).

Additionally, FIA does not support requirements to maintain exit plans for ICT intragroup service providers. ICT intragroup service providers typically share common services, such as general IT services (e.g., server/network/desktop support), risk, (e.g., cyber, third-party risk), finance, legal/compliance, and audit. Financial entities should understand and manage risks associated with their use of intragroup service providers however, given the connected nature between them, these risks need to be managed in a different manner than risks from external third parties. Exiting an intragroup provider may also decrease the operational resilience of the business and fragment the risk management framework used to manage other business risks. As an example, network services (e.g., router/switch/firewall hardware) are generally maintained and operated by the parent organization. Absent of these services, a financial entity cannot sustain its operations, making these services critical. If the financial entity decided to vacate these services to another provider, the decision may impact other services (e.g., application support, finance, compliance) provided by the parent and delivered through this infrastructure. Additionally, by having this service provided by an external party, there is an opportunity to have less consistency in the execution of risk and resilience controls across the financial entity and the parent organization which may lead to a decrease in resilience. Therefore, exit plans for intragroup services may not be effective in all cases and ESAs should consider creating an exception to account for intragroup services.