

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

**Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers**

FIA appreciates the opportunity to comment on the European Supervisory Authorities' (ESAs) first batch of DORA policy products. We support the ESAs aim to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. However, we would like to highlight remaining industry concerns in our responses below.

**Q1: Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?**

Yes. The ITS introduces requirements for financial entities to ensure the provision and maintenance of a valid Legal Entity Identifier (LEI) to identify their ICT third-party service providers (TTPs) and all material subcontractors. This requirement goes beyond current industry requirements and practices and fails to consider the practical challenges of procuring LEIs, particularly across extensive supply chains which often comprise thousands of subcontractors.

Generally speaking, reliance on TPPs to provide appropriate information on their sub-contractors is required. Non-EU based third party providers may not have LEIs or even be familiar with this approach. If TPP is unwilling to adopt this approach, separation of processes by the LE might be required, leading to increased operational risks or reduced market choice. Unfortunately, mandating the provision of an LEI in EU regulation will not, in practice, change this dynamic.

As such, it may simply not be feasible for financial entities to satisfy this mandate and to ensure ongoing validity. At a minimum, ESAs should acknowledge the practical challenges in securing LEIs and consider the time needed to work with service providers to meet the proposed requirements surrounding LEI. We therefore recommend that the requirement be revised to include providing an LEI *if available*. Additionally, the requirement should be applied proportionately and limited to material subcontractors (based on the amended definition we propose in Q2).

**Q2: Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?**

FIA does not fully agree and shares remaining industry doubts and concerns below:



The proposed definition of ‘material subcontractors’ risks an unnecessarily broad scope which does not properly reflect a risk-based approach. The ITS scope broadly considers any subcontractor linked to an ICT service supporting, or supporting material parts of, a critical or important function as a ‘material subcontractor’. However, it is necessary to consider the *role* of the subcontractor and their *potential impact* to the provision of services. This will ensure that the register effectively captures material supply chain risks and relationships that will support the three stated purposes of the ITS, including specifically the objective to identify critical third parties for the oversight framework.

We therefore recommend the definition of ‘material subcontractors’ is amended as follows: ‘material subcontractor’ means a subcontractor of ICT services supporting a critical or important function or providing material parts thereof of the contracted service and whose disruption or failure could lead to a material impact to service provision.

Similarly, the approach to reporting requirements for ICT services that support critical or important functions does not adequately apply proportionate and risk-based principles. Whilst template RT.06.01.0061 appropriately recognises that such arrangements should be subject to enhanced reporting requirements, this approach does not take into consideration the varying levels of risk associated with ICT services supporting a critical or important function – that is, not all ICT services supporting critical or important functions carry a level of risk (or importance) to the financial entity that require enhanced reporting or risk management requirements. Without consideration of the materiality of the ICT service itself, the register will capture an inappropriately broad scope of third-party ICT services and undermine the proportionate and risk-based approach applied to this risk relationships.

We therefore recommend that a Y/N data field is added to template RT.02.02, which is intended to identify whether the contractual arrangement is material to the provision of the contracted ICT service supporting a critical or important function. ICT services that indicate a “Yes” would then be subject to the enhanced reporting requirements. This approach is, in our view, consistent with the Level 1 text and existing registers, and would more effectively support the three stated purposes of the register.

**Q3: Are there any significant operational issues to consider when implementing the Register of Information for the first time? Please elaborate.**

Yes. The maintenance and submission of Registers is an incredibly resource-intensive process that has limited value to internal risk management purposes. The divergence of register requirements across existing outsourcing registers only serves to divert important resources to administrative tasks rather than managing the real risks. We believe that financial entities will not always be able to expand existing registers, to capture the additional information sought, but will have to establish a new database. Proposal is to align and consolidate the various existing registers (e.g., EBA Outsourcing Register). Implementation will require significant resources for the enhancement of tools and remediation of new data requirements of existing vendors.

The templates introduced by the DORA ITS are even more complex and detailed in structure and information requirements. Whilst we acknowledge ESAs efforts in applying a proportionate and risk-based approach, we believe there is further opportunity to streamline data requirements to reduce the reporting burden for financial entities.

ESAs must consider the significant amount of work it will take to establish the first register. The current deadline (January 2025 effective date) is unreasonable and may result in the submission of data that is not high-quality or complete. Acknowledging the implementation deadline imposed by the Level 1 text, we recommend setting the deadline for the first submission **no earlier than January 2026**, or allowing for a phased submission of information that is truly needed to support the supervision and oversight framework objectives of the ITS.

The ITS also requires that financial entities ensure continued validity of the information contained in the register, which is to be updated on an *'ongoing'* basis and received regularly by regulatory authorities. Whilst it is reasonable for financial entities to maintain certain data points on an ongoing basis to support effective ICT risk management practices and processes, it is not practically feasible to secure and validate *all* data points on a constant basis (e.g., outside of recertification exercises or due diligence or assurance assessments). We recommend the ESAs take a risk-based approach to this requirement.

**Q4: Have you identified any significant operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information?**

Yes. If the ESAs' expectation is that this historical information is provided with the first submission of the register (i.e. January 2025), it will not be possible for financial entities to gather all historic data points requested for terminated arrangements as of the date of entry into force.

In view of applying a proportionate and risk-based approach to this requirement, we strongly recommend that a one year period for keeping information from terminated arrangements would be sufficient for satisfying the three objectives of the register. The proposed five year period would entail reporting on a significant volume of information which serves no purpose for achieving the three stated objectives of the ITS.

**Q5: Is Article 6 sufficiently clear regarding the assignment of responsibilities for maintaining and updating the register of information at sub-consolidated and consolidated level?**

**Q6: Do you see significant operational issues to consider when each financial entity shall maintain and update the register of information at sub-consolidated and consolidated level in addition to the register of information at entity level?**

**Q7: Do you agree with the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) in the template RT.02.01 on general information on the contractual arrangements? If not, could you please provide a clear rationale and suggest any alternatives if available?**

No. We struggle to understand the relevance of this information to the ITS objectives and we recommend this data field is removed from the proposed template. Inclusion of this field risks the provision of misleading data which may confuse, rather than inform, the ESAs on any risk considerations. Cost itself is not a driver of the third-party oversight approach and does not change how

we approach our due diligence, nor provide any value on systemic or concentration risks – the management of third-parties requires a risk-based approach.

Furthermore, estimating annual cost/expense for global arrangements with third-parties, i.e. modelling how much of a global service’s spend is relevant just for EU-supervised legal entities at a transactional/arrangement level is a practical challenge as resources are fungible. Estimating this data point at a transactional/arrangement level is also relatively incompatible from an intragroup services perspective. The budgeting of expenses related to intragroup outsourcing services is typically embedded in the annual process at the legal entity level. Furthermore, the cost of outsourcing is not necessarily equivalent with the cost of bringing the activity back in house, or using another provider, so the data point cannot be used to understand the cost of implementing an exit plan.

**Q8: Do you agree that template RT.05.02 on ICT service supply chain enables financial entities and supervisors to properly capture the full (material) ICT value chain? If not, which aspects are missing?**

FIA does not fully agree and shares remaining industry doubts and concerns below:

As per our response to Q2, the focus on a service provider’s supply chain should be on **material subcontractors**, as defined in our response, taking into account their actual role and the potential impact of their disruption.

It is unclear how the ranking of subcontractors provides meaningful information for any of the stated register objectives. Identifying if a subcontractor is a 4th or 6th party does not change oversight or supervision. To support effective risk management and oversight, the register should differentiate between (i) direct third parties and (ii) material subcontractors (based on the proposed amended definition).

**Q9: Do you support the proposed taxonomy for ICT services in Annex IV? If not, please explain and provide alternative suggestions, if available?**

FIA does not fully agree and shares remaining industry concerns below:

Annex IV captures several ICT services that are unlikely to present material risks to some financial entities (FEs) and which are not consistent with the broad definition of ICT services in the Level 1 text. The result will be the reporting of ICT services that do not present the type of risks DORA is intended to address and imposes an inappropriate standardisation and classification of services across financial institutions. It is important that FEs are able to apply a risk-based and proportionate approach under the broad definition of ICT services in determining their reporting obligations.

Specifically, we recommend that the following categories of services are removed from the Taxonomy:

- **S1: Software licensing** – ICT services under DORA should not include an off-the-shelf software license if it is not provided as a service and if it is not provided on an ongoing basis (to be consistent with the definition of ICT service in DORA). An example of this

would be if Microsoft Office is provided via a software licence which the FE could purchase off-the-shelf and install. This should not be an ICT service, compared to Microsoft 365 which is provided on an ongoing basis via cloud hosting. This could meet the definition of an ICT service.

- **S2: ICT Project Management** – ICT Services under DORA should not include provision of a project manager, as a project manager would not be an ICT service provided through an ICT system. If a PMO is provided to an FE outside the context of the provision of an ICT system or hardware, then it is difficult to see how such PMO would be included in the definition of an ICT service. If, however, a PMO is provided to an FE as part of a hardware (or software) provision (e.g. a technical support contact), then the service being provided by that PMO should fall within the definition of ICT service as this would constitute the “technical support via software or firmware updates by the hardware provider” element of the Level 1 ‘ICT service’ definition.
- **S3: ICT Development** – ICT development services, such as software development and testing are typically project-based or provided on a temporary basis, involving the creation or enhancement of ICT systems, rather than the ongoing provision of digital and data services and we do not consider they fall within the Level 1 ‘ICT service’ definition.
- **S16: ICT Consulting** – ICT services under DORA should not include provision of expertise services of an ICT consultant as they do not fall within the Level 1 ‘ICT service’ definition. ICT consulting services which may help FEs make informed decisions about their ICT systems usually entail project-based or advisory engagements, rather than the ongoing provision of digital services through ICT systems.
- **S17: ICT Risk Management and ICT audit** – For similar reasons this category does not fall within the scope of the Level 1 ‘ICT service’ definition. These services are not typically considered ongoing digital or data services through ICT systems and it is otherwise unclear to members what services are intended to be in scope in this category.

**Q10: Do you agree with the instructions provided in Annex V on how to report the total value of assets and the value of other financial indicator for each type of financial entity? If not, please explain and provide alternative suggestions?**

FIA does not fully agree. The relevance of this information to the three stated objectives of the ITS is not clear to us. We would again encourage the ESAs to adopt a proportionate risk-based approach to the register, ensuring that information that is relevant or adds value to risk management and supervision objectives is required, and remove this information requirement.

**Q11: Is the structure of the Register of Information clear? If not, please explain what aspects are unclear and suggest any alternatives, if available?**

Yes. The structure of the Register is clear but we suggest a stronger alignment with existing EBA register requirements. Furthermore, with multiple templates we see a significant level of duplication.

**Q12: Do you agree with the level of information requested in the Register of Information templates? Do you think that the minimum level of information requested is sufficient to fulfill the three purposes of the Register of Information, while also considering the varying levels of granularity and maturity among different financial entities?**

No. The goal of achieving a '*minimum level of content harmonisation*' risks undermining the core objectives of DORA to harmonise regulatory and supervisory approaches across the single market. Additionally, the ITS is silent on whether additional fields could be added by NCAs beyond the ultimate harmonized template. We encourage ESAs to help limit the possibility of further divergence across registers and explicitly restrict any additions to the template by NCAs. Any changes should be approved at EU-level to ensure DORA's objective of harmonized EU framework is maintained.

**Q13: Do you agree with the principle of used to draft the ITS? If not, please explain why you disagree and which alternative approach you would suggest.**

FIA does not agree and shares remaining industry concerns below:

The proposed approach to the 'proportionate' application of the register is flawed and not risk-based. The ITS applies proportionality based on the number of ICT third-party services that the financial entity relies on. This overlooks other essential risk-based factors such as the size and complexity of the legal entity or the criticality of the ICT third-party service provided that are relevant to the application of proportionality based on the risk level of the ICT third-party provider portfolio. We advocate for technical standards that uphold the principle of proportionality by embedding a risk-based approach to the number of data fields and level of information required. We would encourage the ESAs to reframe their approach, ensuring a comprehensive consideration of relevant risks and their proportionate application within the templates.

**Q14: Do you agree with the impact assessment and the main conclusions stemming from it?**

FIA believes clarification is necessary for Policy No. 10. It is uncertain whether the intention is that the register should reflect all contractual arrangements in place by January 2025 (DORA implementation deadline).