FESE response to ESAs consultation on the DORA first batch policy products

11th September 2023

1. Consultation paper on RTS on ICT risk management framework and RTS on simplified ICT risk management framework

1.1. General drafting principles

Q1: Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (Complexity and risks considerations)? If not, please provide detailed justifications and alternative wording as needed.

In considering which financial entities could become subject to more advanced testing, both the principles of proportionality and subsidiarity should be considered, as well as the need to ensure a level playing field. It would not be proportional to make all financial entities subject to the same levels of requirements without distinguishing between their levels of size, type, and criticality to EU markets. However, the size of a financial entity should not be the most relevant metric when determining what cybersecurity requirements ought to apply. Rather, entities should be subject to similar requirements if they have similar risk profiles, including their systemic impact, and whether they conduct similar activities. In general, FESE would caution against overly prescriptive technological measures which would rapidly be outdated due to technological evolution. While there is a need for a coordinated approach to cyber-resilience, when considering further regulatory requirements in this space it is important that flexible innovation is safeguarded since "one size does not fit all". Hence a risk-based and proportionate approach is needed.

Q2: Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.

1.2. Title I: Further harmonisation of ICT risk management tools, methods, processes and policies (Article 15)

Q3: Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

Q4: Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.

Any proposed security risk management framework should be based on internationally developed standards. We believe that the NIST Cybersecurity Framework (CSF) in recent years has become the de facto standard of choice in the financial sector adopted by most financial entities.
Moreover, any requirement to disclose details on cyber resilience should be conducted in a careful manner to ensure sharing of such information does not unintentionally better equip potential attackers, thereby increasing cyber resilience-related risk.

The suggested approach on ICT risk management policy and procedures reflects ESA's comprehensive effort to ensure the security and resilience of financial entities' networks. However, we believe that a slight adjustment could further enhance its precision and overall effectiveness. Specifically, we would like to emphasize the importance of closely monitoring "relevant" or "significant" aspects that may have a material impact on the overall ICT risk profile to ensure an effective and focused approach on the critical aspects for the financial industry as well as for the regulators. Including provisions on the monitoring of "any" changes as described in Article 3 (1)(e) would dilute the scope and focus.

Q5: Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.

The suggested approach on ICT asset management provided in Article 4 is overall in line with our view. One consideration would be about the stipulation given in paragraph 2 point b (ix) which appears to be already covered in paragraph 2 point b (vi). Furthermore, we believe further clarifications are needed on requirements in paragraph 2 point b (vi), namely to list *all* business functions or services supported by ICT assets. We assume it would apply to applications, but it is not clear whether it applies to other elements such as data, network, and energy supplies, among others.

Q6: Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?

FESE agrees that this is an important element as it monitors obsolescence risk.

Q7: Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

While the suggested approach on encryption and cryptography considered in the draft RTS is mostly in line with our view, it could be further improved by recommending that lost, compromised, or damaged keys shall be replaced instead of relying on recovery, as proposed in Article 7 (3), as those keys are overly risky to be recovered. Furthermore, there is a need for clarity in Article 7 (4), to further specify whether the register pertains to only certificates or encompasses keys as well. We believe that these refinements would strengthen the overall framework, ensuring a more robust and secure approach to encryption and cryptographic key management.

Additionally, FESE believes that updating FEs' cryptographic technology "when necessary" in paragraph 50 under the section of 2.3 General Drafting Principles is too broad. "When necessary" should be defined, for instance, as "when recommended by ENISA".

Q8: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q9: Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

Regarding the patch management procedures described in Article 10, we propose that the testing and deployment of software and hardware patches and updates should be conducted in an environment that does not entirely "replicate" but is instead "very close" to the production one, as some minor differences (e.g., fewer memory capacity) would not cause any disruptions on the testing process. The requirement as proposed would lead to increased complexity and limit flexibility.

Moreover, the synchronisation of clocks requirement, encompassed in the logging procedures proposed in Article 12, should be limited and tailored exclusively to ICT systems serving important and/or critical services. By adopting this focused approach, it could be ensured that critical operations receive precise focus and timestamping while optimizing resource allocation across the organization and thus ensuring financial stability.

Q10: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q11: What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.

Q12: Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.

Q13: Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.

The suggested approach on network security, particularly the emphasis on network security management and the encryption of network connections to safeguard against intrusions and data misuse in Article 13, is deemed comprehensive. However, from a trading venue perspective, co-location services play a critical role in reducing latency and ensuring competitive operations. Technological development has allowed the establishment of low latency environments in global trading landscapes. Market participants are involved in those low latency environments, allowing markets to grow. The rule as proposed would lead to a massive impact on latency and, thus, on trading characteristics which would put Europe at a disadvantage compared to other trading landscapes globally (e.g., UK, USA). We suggest inserting another sentence which would

emphasize on certain exemptions being possible with regard to communication within the same data center.

Q14: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q15: Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

Q16: Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.

FESE believes that specific elements regarding supply-chain risk should not be taken into consideration in the RTS.

Q17: Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.

Q18: Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

Q19: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

FESE believes that no new measure or control should be taken into consideration in the RTS in addition to those already identified.

Q20: Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

FESE agrees with the suggested approach regarding ICT and information security awareness and training.

Q21: Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion

FESE agrees with the suggested approach on Chapter II – Human resources policy and access control.

Q22: Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

FESE believes that no new measure or control should be taken into consideration in the RTS in addition to those already identified.

Q23: Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.

FESE agrees with the suggested approach regarding ICT-related incidents detection and response.

Q24: Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

The proposal put forward with regards to ICT business continuity management, including the specific considerations for CCPs, CSDs and trading venues, does not reflect nor align with the exchange perspective. Firstly, various concerns emerge regarding the feasibility of maintaining identical secondary processing sites with distinct geographical risk profiles. It should be taken into consideration that the Recovery Point Objective (RPO) in regard to data loss is required to be close to zero, which can hardly be achieved in the setup indicated in the proposal. Coping with the 'different geographical risk profile' requirement is therefore limited by the RPO.

In addition, to ensure orderly markets, order data is being purposely deleted. A fresh order book would allow the market to take new information into consideration and therefore add new trading interest into an order book rather than confronting market participants with the order book outdated information.

Lastly, with regard to the testing of the ICT business continuity plans outlined in Article 26, it is imperative to introduce a mitigating opening clause in order to prevent any adverse repercussions on the trading venues' business and operational landscape. For orderly trading to take place on trading venues, it needs to be considered that technological developments allow low latency trading in which many market participants globally engage. The proposal put forward would severely impair the way trading is performed globally, as it would add massive latency.

Also for Q25.

Q25: Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

FESE considers that a one-size-fits-all model for duration and recovery would not be suitable. Moreover, any regulatory measures in this space would need to be sufficiently broad to allow flexibility to new types of situations and issues, recommending specific and quantitative parameters should thus be avoided. It is very important that different approaches, in line with the different needs of exchanges, are allowed. Exchanges avail of a number of mechanisms to safeguard trading and price discovery and their discretion should not be limited by overly prescriptive regulatory measures when it comes to the functional design, application and interplay of cyber-resilience measures. FESE considers that the RPO should be the point in time when the market operator is comfortable that it can ensure again a fair and orderly market. On a general basis, financial market infrastructure operates under a 2-hours RTO guidance, as per CPMI-IOSCO Principles of Financial Market Infrastructure. 2-hours RTO guidance works well under operational disaster recovery plans, but we consider that mandating RTO under specific legislation

would be counterproductive. Furthermore, exchanges have in place outages standard protocols tailored to different markets. DORA should take this into consideration.
FESE understands the need for maintaining a “secondary site”, however, the requirements outlined in the RTS might not be necessary as the purpose of maintaining the secondary site could be fulfilled by working from home.
Additionally, the requirement for testing of ICT TPP, outlined in Article 26(2)(c), will narrow down the scope of ICT TPPs to a very selected number of critical ICT TPPs that can satisfy the requirement of switchover of critical business functions. FEs should have the possibility to make the test in 2 parts, one internal and one external. These tests should not be required to be performed simultaneously as it could be too difficult to coordinate.

Q26: Do you agree with the suggested approach on the format and content of the report on the ICT risk management framework review? If not, please explain and provide alternative suggestion.

In regard to the suggested approach on the format and content of the report on the ICT risk management framework review highlighted in Article 28, there is a need for clarity, particularly in paragraph 2 point a (iii). Article 6(5) of DORA entails that the "ICT risk management framework shall be documented and reviewed at least once a year," and reviewed by independent auditors. The proposed RTS stipulates a detailed report that appears to mirror the content of the framework, resulting in duplicated requirements. If a company has a stable framework (yearly reviewed and audited), a report on possible deltas should be considered sufficient.

1.3. Title II : Simplified ICT risk management framework

Q27: Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.

Q28: Do you agree with the suggested approach regarding the further elements of systems, protocols, and tools to minimise the impact of ICT risk under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary

From a trading venue perspective, co-location setups play a critical role in reducing latency and ensuring competitive operations. As highlighted in Q13, technological developments have allowed the establishment of low latency environments in global trading landscapes. Market participants are involved in those low latency environments, allowing markets to grow. The rule as proposed would lead to a massive impact on latency and, thus, on trading characteristics which would put Europe at a disadvantage compared to other trading landscapes globally (e.g., UK, USA). Therefore, we would like to emphasize on the need for an introductory clause in Article 37 (1) and (2) explicitly considering these imperatives. By doing so, the implementation of security measures can be harmonized with the low latency imperative and future trading developments but also overall ICT risk impact while pursuing efficient financial activities.

Q29: What would be the impact for financial entities to expand the ICT operation security requirements for all ICT assets? Please provide details and if possible, quantitative data

Q30: Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples

Q31: Do you agree with the suggested approach regarding ICT business continuity management under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

Q32: Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.

2. Consultation paper on RTS on criteria for the classification of ICT-related incidents

2.1. Classification criteria and thresholds of major incidents

Q1: Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.

For cyber incidents, there are two factors which should be considered as relevant in determining the materiality thresholds: Was the incident impactful? Was the incident caused by a threat actor who had a targeted and malicious intent?

Using the criteria above, only incidents that are both impactful and have targeted and malicious intent should be considered as reportable.

It is important to keep in mind that incidents that do not have a material impact can be important for intelligence sharing among financial entities to align protection activities. If the reporting is done only if there is a material impact, it would filter out attacks that were unsuccessful in one case but can succeed with the second attempt with another entity. The attack could also be successful but not have a material impact on the critical functions of one financial entity but can have a material impact on another entity that has different protection mechanisms. It could be useful that financial entities are informed about such incidents and this information is used as a source of Threat Intelligence. Therefore, the Commission should explore the possibility of having a mechanism for the collection and reporting of these incidents, in an anonymised manner and made available for financial entities to align their protection activities.

We also believe that quantitative measures should be taken into account to identify criticality. The frequency of an incident should not impact its criticality level. The causes should be investigated but the qualification should not change, and it should not be reported to authorities.

Q2: Do you agree with the specification and materiality thresholds of the criterion 'Clients, financial counterparts and transactions affected', as proposed in Articles 1 and 9 of the draft RTS? If not, please provide your reasoning and suggested changes.

Q3: Do you agree with the specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS? If not, please provide your reasoning and suggested changes.

We do not agree with the classification criterion on "Duration and service downtime" outlined in Article 3. Incidents on non-critical processes should not be defined as critical based on downtime. The last sentence of the paragraph in Article 3(1) is critical and the interpretation of the sentence should be confirmed: "Finally, since it may be challenging for FEs to identify the actual moment when the incident will be resolved, the draft RTS envisages that FEs can resort to estimates".

The "geographical spread" threshold, outlined in Article 4, that requires FEs to assess the impact of the incident in at least two Member States appears to be quite low.

Furthermore, we believe the specification in Recital 11 that "all details" of the incident should be covered in the report to competent authorities is too broad. There should be a summary of the incident, the root cause and the action plan.

Q4: Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes.

FESE agrees with the specifications and threshold of the criterion "Data losses", as proposed in Article 5.

Q5: Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes

We do not agree with the specifications included in Article 6. "Critical services affected" should be services that contribute to the main financial health of the company and that support the health of the clients, and ICT services that support those services.

Additionally, we believe the discarded alternative approach of leaving to the FE the discretion of assessing the critical services based on existing BIA would make more sense considering the point made in paragraph 45: considerations on whether to escalate the incident to senior management depend on the impact on critical services as per the FE's own BIA, so this would create a discrepancy between the criteria for senior management reporting and the ones for regulatory reporting.

Q6: Do you agree with capturing recurring incidents with same apparent root cause, similar nature and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes. Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents)

Q7: Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.

Q8: Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes.

3. Consultation paper on RTS on the use of ICT services supporting critical or important functions provided by ICT third-party service providers

Q1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?

Q2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

Q3: Is article 4 appropriate and sufficiently clear?

Q4: Is article 5 appropriate and sufficiently clear?

Q5: Are articles 6 and 7 appropriate and sufficiently clear?

Q6: Is article 8 appropriate and sufficiently clear?

Q7: Is article 9 appropriate and sufficiently clear?

Regarding the selection of Option A for the Policy Issue 7 on Contractual clauses (i.e., page 25), we would like to highlight the difficulty that ICT service providers of standard IT services (e.g., Hardware maintenance, software development tools, etc.) may encounter to implement this requirement.

Q8: Is article 10 appropriate and sufficiently clear?

Q9: Is article 11 appropriate and sufficiently clear?

When considering the exit and termination of contractual arrangements for the use of ICT services supporting critical or important functions, as outlined in Article 11, we support and agree with the exit plan periodic review requirement. However, we emphasize that

the periodic testing of the exit plan would be hardly feasible from an execution perspective (i.e., conducting the actual testing and not only analyzing if testing is still possible).

Moreover, considering the statements made in Policy issue 3, item 27 (page 23), for existing contracts where such exit plans do not already exist, we suggest that a certain adjustment period shall be granted in order to establish and implement those required exit plans.

4. Consultation paper on ITS to establish the register for information

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?

The provision given in Recital 10, and further developed in Article 4(7),(8), emphasizing on the distinction between national codes or company names and the distinct advantage offered by the legal entity identifier (LEI) for unambiguous identification of financial entities and ICT third-party service providers. However, it is crucial to acknowledge that not all third-country ICT providers may possess or provide trading venues with an LEI, requiring a strong consideration of additional or alternative criteria, such as for instance Tax ID, to facilitate a comprehensive and effective identification mechanism.

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?

The stipulation made in Article 4(1)b is in line with our view. However, paragraph 1(a) appears to encompass a wide range of ICT service types, necessitating a refined and narrowed-down scope that closely focuses on pertinent and applicable ICT services. Additionally, we recommend the exclusion of standard IT services such as hardware maintenance and standard software licenses. This review must also be considered for Recital 8.

There has been progress of ESAS to designate in accordance with some quantitative/qualitative metrics the qualification of Critical ICT service providers (Article 31 DORA). We believe the first rank should be qualified as they are directly responsible of providing the service to the Financial Entities. We also understand a supply chain overview. Nevertheless, we highlight that the definition of critical functions (Article 3 (22) DORA) and the term "material subcontractors" could be open to interpretation, which can lead to inconsistencies in how the requirement is applied and may lead to: (i) over usage to qualify subcontractors that may not be material to the Financial Entity (with all the consequences of the application of the requirements to a subcontractor that at the end is not material) (ii) under usage of the qualification which at the end is the Financial entity that will liaise with the direct relation which is Rank 1 that needs to adopt the corrective measures on the service provided to the FE. Nevertheless, we recommend providing more specific definitions or guidelines on what constitutes a "material subcontractor" and a "critical or important function". This would help ensure that the provision is applied consistently and effectively across the financial entities with the same business models.

Finally, as we read the subcontractors as those ICT third-party providers being counterparties of a direct ICT third-party service provider, we believe that it should be specified for the sake of clarity that subcontractors of subcontractors and so on are out of scope and shall not be included in the Register.

Q3: When implementing the Register of Information for the first time:

- What would be the concrete necessary tasks and processes for the financial entities?
- Are there any significant operational issues to consider?

Please elaborate.

When implementing the Register of Information for the first time, trading venues falling in scope of this new requirements would first need to introduce and implement necessary pre-requisites, tasks and processes such as establishing and/or adapting an application to create and maintain the templates of the register as well as compiling and further enriching the required data.

With regards to the required changes and updates of the information contained in the register of information (i.e., Article 4(3)), we strongly encourage the replacement of "on-going" basis by a different term for this provision to be achieved for all considered information. While we agree with the proposal on updating the register of information, conducting those updates on a "regular basis", for instance, every six months, is deemed more appropriate in order to reduce complexity and enhance efficiency.

We also believe implementing the register at the consolidated/sub consolidated view, within all entities will be complex, inefficient and extremely time-consuming. In addition, capturing up-to-date, accurate information on the supply chain could be challenging and difficult to maintain.

It would be important to provide clear guidelines and a first phase of support to financial entities to help with the implementation of the Register of Information effectively and efficiently to minimize the risk of inaccurate or wrong information populated in the Register.

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?

The main obstacles could relate to increased costs on data storage, and, as regards existing agreements, compliance with the retention period already authorised by these arrangements.

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?

We believe having a register per entity would multiply the information, and create a risk of desynchronisation and inconsistencies, not to mention that as regards financials, the information can only be reported at the consolidated level.

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

We believe that maintaining and updating registers at multiple levels add a layer of complexity to the data management process and data consistency which can be more challenging when managing registers at different levels.

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?

With regards to the template RT.02.01 on general information on the contractual arrangements, we strongly disagree with the proposed inclusion of columns RT.02.01.0041 and RT.02.01.0042. The rationale underlying this disagreement stems from the substantial increase in complexity that would arise following the inclusion of those columns, especially in the context of intercompany service provisions and their intricate organization. In light of our concerns and in order to lower complexity and ensure a comprehensive and effective representation, we suggest either excluding intragroup transfers from the scope or, alternatively, incorporating specific language that explicitly provides an exemption in such cases.

It is important to point out that we support this approach only at the consolidated level but would not support this approach being applied at the individual entity level.

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?

Template RT.05.02 on ICT service supply chain would not enable financial entities and supervisors to properly capture the full (material) ICT value chain. The completeness and effectiveness of this template would fully rely on the information obtained from the ICT service providers and their engagement and collaboration.

Considering that (i) the Financial Entity is the primary responsible towards its clients to provide quality services, (ii) the ICT Rank 1 is accountable towards the Financial Entity and is obliged to oversee the services that it has sub-outsourced (sub provider) and (iii) the NCAs will oversee the Financial Entities and their ICT 'Rank 1' providers, we believe that the material aspects are already covered. On the other hand, we believe each ICT provider is better placed to provide such information of the sub-providers. We understand it is important to balance the need for comprehensive information with the practicality and manageability of the Register for financial entities.

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

Generally, we support the proposed taxonomy, however, it could be beneficial to provide more detailed descriptions for each service (eg. specifying if maintenance services are included, for each ICT service name which IT components it includes, and if it includes solely hardware, software, simple intellectual property services, or all together and addressing simple hosting (data center) and provision of AI tools). Finally, we highlight that the ICT landscape is constantly evolving, and new types of services and technologies are continually emerging. Therefore, the proposed taxonomy may turn outdated.

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?

The report of statutory accounts is already disclosed by Financial Entities to their NCAs. We believe annual/bi-annual accounts reported to NCAs provide the information already required and should not be under the scope of this Register.

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

The structure of the Register of Information is considered sufficiently clear.

When considering the access of competent authorities to the Registers of Information, the provisions described in Article 9 (1) require additional refinement and clarification. While we agree with the importance for competent authorities to access the information from the Register, a more precise description of the frequency at which the regulators shall receive this information is required to allow for effective implementation. We would suggest that this information is provided on a yearly basis as this has already been proven to be effective and efficient under other regulations (e.g., MiFID II – MiFIR).

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?

The level of information requested in the Register of Information templates is generally deemed sufficient. Comparing the register under outsourcing rules and these templates, it is easy to conclude that these templates have an extreme level of granularity on the information to be provided. Furthermore, we do not see the relevance of collecting such a level of information that goes far beyond what is requested under DORA level 1 (Article 30) or in the current outsourcing rules applicable to the Financial Sector. Additionally, considering the retroactive effect in Article 4 (4) the ITS should have a transitional phase in the period for agreements in force in respect to the information requested in the templates. The complexity of populating the register, especially with reference to pre-existing contractual arrangements, should be taken into consideration.

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.

Q14: Do you agree with the impact assessment and the main conclusions stemming from it? In addition to the consultation questions above, for each column of each template of the register of information, the following is asked:

a) Do you think the column should be kept? Y/N

b) Do you see a need to amend the column? Y/N

c) Comments in case the answer to question (a) and/or question (b) ”No”.

The impact assessment put forward in this proposal raises major concerns as it would entail a substantial increase in the overall efforts for financial entities. To reduce its complexity, it is necessary to further refine the proposal while taking into account the propositions and feedback emphasized in the previously answered questions.

With regards to the templates RT.02.01 on general information on the contractual arrangements, we recommended the amendment of certain columns.

Firstly, either column TR.02.01.0060 or columns TR.02.01.0071, TR.02.01.0072, and TR.02.01.0073 (i.e., Annex I, page 41 & Annex II, pages 77-78) shall be considered "mandatory" components. The columns TR.02.01.0071, TR.02.01.0072, and TR.02.01.0073 should serve as a comprehensive solution for all instances involving ICT service providers without an available Legal Entity Identifier (LEI). This approach would be consistent with template RT.05.01 on ICT third-party service providers, specifically columns RT.05.01.0010, RT.05.01.0021, RT.05.01.0022, and RT.05.01.0023 (i.e., Annex I, page 47 & Annex II, page 91), which exemplify a commendable practice in accommodating scenarios where an LEI is not available.

A similar approach is advocated for the RT.05.01 templates, where either column TR.05.01.0090 or columns TR.05.01.0101, TR.05.01.0102, and TR.05.01.0103 (i.e., Annex I, page 49 & Annex II, pages 93-94) should be designated as "mandatory". These columns, namely TR.05.01.0101, TR.05.01.0102, and TR.05.01.0103, would sufficiently address situations where an LEI is not available, mirroring, once more, the approach established in the columns RT.05.01.0010, RT.05.01.0021, RT.05.01.0022, and RT.05.01.0023 described on page 47 of Annex I as well as page 91 of Annex II.

Although we understand the purpose of the Register of Information, we note that:

5. The ICT Services under the scope are extended to include not only ICT outsourcing but all ICT services;
6. The information requested is far more granular than the one foreseen in the Register applicable for Outsourcing rules besides the overlap of different Registers;
7. To maintain and keep the information updated will require significant resources and additional costs to the Financial Entities;
8. Information that is already disclosed to NCAs under other Regulations should not be included in the Register of Information eg. Statutory Accounts;
9. Information that can be rapidly outdated or that other entities are better placed (eg. External ICT providers) to provide such information should not be reflected in the register of information, eg, the details of the Ultimate Parent Undertaking of the ICT Service Provider or on Sub providers.