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

4th March 2024

1. Consultation Paper on draft RTS and ITS on major incident reporting under DORA

Q1: Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

The proposed timelines for the submission of the initial notification and final report, as provided in Article 6(1) points (a) and (c), are clear and reasonable from the trading venue perspective.

With regards to the intermediate reports (i.e., Article 6(1) point (b)), while we agree with the first limit of "72 hours from the classification of the incident as major", we would like to point out that the current proposal does not consider timelines for the submission of the intermediate report "after regular activities have been recovered and business is back to normal", implying that such report updates must be submitted immediately after activities are recovered. Therefore, to enhance clarity and ensure consistency with the other timelines, we suggest that time limits should be explicitly provided for financial entities to submit these intermediate report updates. The considered time limits shall also be sufficiently broad to allow financial entities to ensure the good quality of the submitted information.

Considering all these aspects, we suggest the following changes to Article 6 (1) point (b):

"b) an intermediate report shall be submitted within 72 hours from the classification of the incident as major, or ~~***when***~~ ***as early as possible within 4 hours after*** *regular activities have been recovered and business is back to normal."*

Further, we do not agree with the following requirement as we see a risk of overreporting:

According to DORA Art. 19.4 (b) 'as soon as the status of "the original incident has changed significantly" or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority'.

The RTS does not provide further clarification as to what 'significant' change is and when we have to send an intermediate report. Additionally, an intermediate report requires a lot of information to be reported.

Finally, we consider that Article 6(2) on the submission of the intermediate and final reports that fall on weekends and bank holidays should also be applicable to the initial notification. It is crucial to point out that employees who create or approve reports are not the same people who detect and resolve incidents.

Q2: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The suggested data fields presented in the draft RTS and the Annex to the ITS for the initial notification of major incidents under DORA are generally acceptable, with the exception of the financial fields and fields that concern impact on external parties, which pose a greater challenge considering the short timelines and availability of information.

For instance, 2.8-2.10 fields of Annexes I and II concern the potential impact on external parties. In case of a major ICT-related incident, the focus during the initial phase after discovery is and should be internal damage control and containment. It is not likely that the full impact on other entities and/or third-party providers is available at an early stage and premature information could be misleading. Therefore, it is prudent to include this information in the intermediate report when a proper assessment has been made.

We also would like to point out that the legal entity identifier (LEI) can provide numerous benefits for the 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.

Finally, in Article 3 (j) on the content of initial notifications, we suggest including after "(j) Other information" the following clarification: "where sensible". Article 3(j) would read as follows: "A) Other information where sensible."

Q3: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The suggested data fields presented in the draft RTS and the Annex to the ITS for the initial notification of major incidents under DORA are generally acceptable, with the exception of the financial fields and fields that concern impact on clients, counterparties and transactions, which pose a greater challenge considering the short timelines.

For instance, 3.6 - 3.12 fields of Annexes I and II concern the impact on clients, counterparties and transactions. In case of a major ICT-related incident, the focus during the initial phase after discovery is and should be internal damage control and containment. Due to the volume and complexity of trading and clearing, it may take more time to evaluate and report the impact. An early assessment might not be as detailed or complete as required and therefore, it might not provide much value.

We would like to further point out that the data field 3.13 (Value of affected transactions) in Annex II of the draft ITS (page 44) does not allow financial entities to estimate the value of affected transactions based on available data in case the actual value cannot be determined. The instruction provided in this data field appears to be contradicting the requirements set in Article 1(5) and 9(2) of the RTS on the Classification of ICT-related Incidents (part of the first batch of DORA policy products), which stipulates: "Where the actual number of clients, financial counterparts or number or amount of transactions impacted cannot be determined, the financial entity shall estimate those numbers based on available data from comparable reference periods."

As we mentioned earlier, the financial fields pose a greater challenge considering short timelines. Therefore, in order to align with the aforementioned requirement, we suggest adding "Where the actual value of transactions impacted cannot be determined, the financial entity shall use estimates" to the instruction section of the data field 3.13, which would then also align with the data field 3.11 (Number of affected transactions). Following these amendments, the description of the data field 3.14

(Information whether the numbers are actual or estimates) shall be changed accordingly, i.e., "Information whether the values reported in the data fields 3.5. to 3.12 3.13 are actual or estimates".

Finally, 3.40 field of Annex II on pages 63-64 requires some data that exchanges will not be able to provide for privacy reasons. For example, exchanges will not provide the email address (of the recipient) or the login username of their users. Therefore, we encourage the ESAs to remove these requirements from the list for privacy reasons.

Q4: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

The suggested data fields presented in the draft RTS and the Annex to the ITS for the initial notification of major incidents under DORA are generally acceptable, with the exception of the financial fields, which pose a greater challenge considering the short timelines and the level of detail they require.

For example, 4.14 – 4.25 fields contain too many details on financial impact and they should not be reported. We would like to emphasise that financial impact details should be reviewed and subtracted to more core/mandatory information (all categories compile to a relatively large number of details). Meanwhile, we consider that reporting on gross costs and losses as in 4.14 is relevant.

Q5: Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes

The suggested data fields presented in the draft RTS and the Annex to the ITS for the initial notification of major incidents under DORA are generally acceptable, with the exception of the financial fields, which pose a greater challenge considering the short timelines.

We would like to point out that the definitions of "significant cyber threat" and "cyber incident" seem to be perplexed. "Cyber threat" would indicate potential danger or malicious activity, while a "cyber incident" is an actual occurrence or event that compromises the security of information assets. Additionally, the template fields are requesting too much information.

Furthermore, it doesn't allow an option for sharing a cyber threat (potential danger or malicious activity) anonymously. For example, some exchanges are members of the CIISI-EU forum, where companies share information on cyber threats on a monthly basis and they are allowed to share the information anonymously. As a result, it poses an important question of where the reports under DORA would be stored in terms of confidentiality.

Finally, we consider that the ESAs should make use of already known frameworks (i.e. NIST SP 800-150 or CISA) for sharing and reporting cyber threats which most of the companies already follow.

Q6: Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

2. Consultation Paper on draft GL on costs and losses

Q1: Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

Q2: Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

It may be burdensome to keep tracking various costs related to an incident in particular for those costs and losses that could materialize a long time after the incident was closed. For instance, a claim by a customer for damages caused by an incident. The purpose of this reporting and the impact on internal monitoring and reporting accounting systems appears disproportionate.

Q3: Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

3. Consultation Paper on draft RTS on thread led-penetration testing (TLPT)

Q1: Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed.

Q2: Do you agree with this approach [*proportionality approach to identify entities to perform TLPT*]? If not, please provide detailed justifications and alternative wording as needed.

Yes, in general, we support the proportionality principle with the emphasis that any attempt to avoid requirements by declaring "Pseudo-insignificance" should be prevented. However, concerning trading venues, we do not see that the proportionality approach is fully respected. With reference to our answer to Q4, we would prefer a scope that is not too broad and covers only trading venues that are truly systemically important.

We also would like to emphasize that size should not be the main metric when determining cybersecurity requirements. Rather entities having similar risk profiles should be subject to similar requirements.

Q3: Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.

Q4: Do you agree with the proposed quantitative criteria and thresholds in Article 2(1) of the draft RTS to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.

We do not agree with the proposed quantitative criteria and thresholds for trading venues in Article 2(1)(f) of the draft RTS. While we fully appreciate the necessity to carry out TLPTs by financial entities that are large or interconnected enough to have a systemic impact, we do not see that the proposed criteria for trading venues reflect the systemic character enough.

The criteria, especially at the national level, are too broad and could cover entities that are not systemic in nature, thus leading to a disproportional burden. For example, the highest market share in terms of turnover in a specific financial instrument class is not a proper criterion. In national markets where competition is high – such as in Germany – there may be in some financial instrument classes no trading venue that has a significant market share of 70% or more. It could lead to a comparative disadvantage, if a trading venue with a market share of 35% fell under the requirements of the RTS to carry out TLPTs, but the second largest trading venue with 30% would not. That would be an unreasonable advantage for the latter, as this venue would not fall under the requirement to perform TLPTs.

Furthermore, not every asset class is systemic by nature, meaning that if trading in such asset classes in the venue with the highest market share is interrupted due to IT-related attacks, it is not automatically a critical event for the entire financial system or society. This is especially true for secondary market trading venues, where the functionality of price formation can also be performed by other venues, thus reducing even more systemic impact. That should be considered when defining the quantitative criteria. A more suitable criterion could be one that does not distinguish between different financial instrument classes but considers the highest market share of a venue across all asset classes. Additionally, Article 2(f)(i) should also have absolute figures as a criterion, in case

there exists only one national trading venue or only Article 2(f)(ii) should be applicable in this case.

Nonetheless, we support the possibility laid out in Article 2(2) that financial entities shall not be required to carry out TLPTs when an assessment of the TLPT authority that considers the impact of the financial entity, financial stability concerns or the ICT risk profile do not justify the performance of the test.

Q5: Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions.

No, we consider the RTS to sufficiently reflect the main aspects of TIBER-EU.

Q6: Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT? If not, please provide detailed justifications and alternative wording as needed.

Yes, in particular, we see it as imperative that the top management must approve the potential risks that stem from conducting TLPTs.

Q7: Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed.

We would like to point out that the requirements for external testers are very comprehensive and may not be fully controllable in practice. TLPTs are usually carried out by a large team, and it is difficult to verify the experience of all testers. Or there may be a lack of certificates and, thus, a limited availability of eligible testers. Furthermore, not every provider of such tests is likely to have insurance that covers TLPT activities, as the risk is very high, and costs could quickly exceed the value of the company. It is important that the company carrying out the test has a good reputation and good references. Those are the most important factors listed in Article 5, from our point of view.

Additionally, requesting three and five references from previous assignments related to intelligence-led red team tests poses challenges. The nature of such engagements often demands a high level of confidentiality to preserve the effectiveness of the assessments. Disclosing specific details about prior assignments could compromise the anonymity and security of the clients involved.

Finally, organisations seeking such services may face challenges finding vendors with a well-established track record in the relatively new domain of threat-led penetration testing in the EU cybersecurity landscape.

Q8: Do you think that the specified number of years of experience for external testers and threat intelligence providers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills? If not, please provide detailed justifications and alternative wording as needed.

The specified number of years of experience for external testers and threat intelligence providers assigned to the TLPT (as provided in Article 5(2) points (e) and (f)) is not an entirely appropriate measure to evaluate the staff's knowledge and skills and will present difficulties in finding the right external vendors, with such experiences. It would highly increase the cost of the overall Threat-Led Penetration Testing.

To provide more flexibility, we would suggest replacing the "number of years of experience" criteria with "sufficient expertise", as we strongly believe that financial entities shall be able to decide, after conducting a thorough selection process and assessment, if the external testers and the staff of the threat intelligence provider assigned to the TLPT have a sufficient and appropriate qualification and therefore satisfy the expertise requirement. Please also refer to our answer to question 7.

Q9: Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed.

We would like to raise key concerns regarding the proposed process on the performance of threat-led penetration tests, as provided in Chapter III of this RTS.

Firstly, related to the testing environment – we believe that conducting the tests on live production systems presents unacceptable risks with potential negative impacts not only for the trading venues and their trading systems, but also for trading participants and financial entities depending on continuous price information.

In general, financial entities and particularly trading venues are required to "ensure a strict separation between the testing and the production environment or permit testing only out of trading hours" (i.e., RTS specifying organisational requirements of trading venues under MiFID II). As the threat-led penetration tests are required to be conducted on live production systems already under Article 26 of DORA, we believe that financial entities must at least be granted more flexibility and discretion to determine the moment and time deemed most appropriate to perform the tests – for instance during non-critical/core operating hours. This is an essential aspect to consider in order to minimise the potential for risks and avoid significant disturbances and negative impacts on the business and operations of trading venues.

Secondly, the proposed RTS stipulates that the testing process shall be conducted for a duration of 12 weeks. We would like to point out that, due to this set duration, the performance of these tests will become highly complex in case multiple trading venues, that are running on the same trading system, are required to perform the testing process by the TLPT authority at the same time. From our perspective, it would be highly beneficial for financial entities to be able to cluster these tests above the group level, thus allowing entities that use common trading systems or the same ICT service providers to conduct the tests jointly. This would reduce complexity and enhance efficiency. We would also call for more discretion on the timeframes.

We would also like to comment on the following provisions proposing some amendments:

- Article 6(1) provides that the financial entity shall submit the initiation documents to the TLPT authority within three months. We consider that 3 months' notice seems to be too short. TIBER-EU Framework provides a longer time notice of almost 12 months and we propose to keep the same requirement.
- Article 7(3) states that the control team chooses the scenario themselves. Based on the TIBER framework, the Threat Intelligence team comes up with the scenarios together with central banks. It would be beneficial to have the same requirement.
- We consider that in Article 8(5), the duration of the active red team testing phase shall be a minimum of twelve weeks and a maximum of 16 weeks.
- Article 9(7) provides that the control team shall submit the test summary report to the TLPT authority for approval within 12 weeks from completion of active red team testing. The TIBER Framework provides 16 weeks and we consider that the requirement should stay the same.

- Article 10 (2c, 2d) states that the remediation plan must provide information on - root cause analysis and the financial entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements. These requirements are asking companies to provide highly sensitive information. We encourage the ESAs to consider making changes for this specific reason.

Q10: Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.

While we overall agree with the proposed requirements for pooled testing, one aspect is lacking clarity from our perspective. In order to reduce complexity and ensure more flexibility, we believe that financial entities not belonging to the same group shall be able and allowed to conduct pooled testing jointly, as long as these entities are using common ICT systems or the same ICT service providers. To enhance clarity, we suggest explicitly including such a provision in Article 12 of the draft RTS.

Q11: Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.

We disagree with the requirement from Article 11, paragraph 1(a) under ii that internal testers have to be employed by the financial entity or by an intragroup service provider for the preceding two years. This requirement could be counterproductive for financial entities hiring IT/cyber talents and also from internal workload capacity.

Q12: Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.

Q13: Do you have any other comment or suggestion to make in relation to the proposed draft RTS? If so, please provide detailed justifications and alternative wording as needed

We would like to suggest the regulators provide specific guidance on the classification of TLPT Reports and how it is going to be authorised. We believe it is crucial to avoid misclassification of these reports.

4. Consultation Paper on draft RTS subcontracting

Q1: Are articles 1 and 2 appropriate and sufficiently clear?

No, Article 2 is (a) not sufficiently clear, and (b) establishes responsibilities which contradict company law.

Ad (a) it is unclear where the RTS applies "on a sub-consolidated or consolidated basis", as the RTS applies to financial entities and not groups of entities.

If the target of Article 2 is to establish responsibilities of a parent undertaking for its sub-consolidated or consolidated affiliates, this should be clearly stated, e.g. "Where this Regulation applies to financial entities which are consolidated or sub-consolidated by a parent undertaking, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group shall ensure, that the conditions for subcontracting (…)". The reference "where permitted" does not imply which permission is meant and is thus unclear. Is this a permission by a group entity provided to the parent undertaking (in case of outsourcing to the parent undertaking), or is this a reference to a permission of the parent undertaking to its subsidiary to allow its ICT third party service provider to use subcontractors? As the RTS only governs subcontracting, we deem the "where permitted" may be superfluous.

Ad (b) Article 2 assigns responsibility to the consolidating parent undertaking for the consistent application of the Regulation in the ICT contracts of its consolidated subsidiaries. Ultimately this means assigning managerial liability to the directors of the parent company for the compliance of its affiliates in the field of ICT subcontracting.

This is not mandated by the first level regulation, DORA only entitles the ESA to "develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions." paragraph 2, point (a). Art. 30 paragraph 2 point (a) sets out certain requirements for ICT contracts and does not make any reference that may imply any assignment of responsibility to parent undertakings of a financial entity. Such assignment is neither an element of "assessment" by the financial entity, nor may the financial entity "determine" a third party responsibility for its own actions (contract to the detriment of a third party).

In many cases, the parent undertaking does not have any legal right or means to influence the day-to-day business of its subsidiary, e.g. if the subsidiary is a publicly listed company. Assigning legal responsibility to the parent undertaking for subsidiaries, that it cannot steer in their day-to-day business appears to be inappropriate. It remains unclear how the elements of increased or reduced risk affect the requirements of Articles 2 to 7.

We would like to also point out that the principle of proportionality seems not applicable throughout the RTS. The expected level of monitoring by the FE of subcontractors is high, and we believe it is disproportionate and challenging to implement. We question the balance of these provisions as a lot of insight into the level of the third party's business set-up is expected of financial entities. The new provisions will shift the burden towards the financial entity where, currently, this level of responsibility is agreed on in the contract where financial entities are relying on the responsibility and liability of the third party to honour the terms of the agreement. This balance may be distorted by the severity of the Draft RTS provisions and may lead to a disbalance that does not represent the individual responsibility of the contracting parties.

Taking everything into account, we believe that Article 2 is excessive and goes beyond the delegation to ESAs as set forth in Article 30 (5) DORA. The delegation to ESAs only refers to the further specification of elements when subcontracting is permitted and the conditions applying to such subcontracting. This does not include any reference to the specification of financial entities' obligations in relation to their subsidiaries. We

therefore believe that Article 2 shall be removed from the Draft RTS and it shall only include the conditions as set forth in Article 30 para. 2 (a) and para 5.

Q2: Is article 3 appropriate and sufficiently clear?

Firstly, Article 3 implies far-reaching due diligence requirements to be fulfilled before agreeing to a subcontracting of critical functions. The definition of ICT third party services was broadened compared to the definition of "ICT Services" in DORA to also cover e.g. software licenses and ICT consulting.

As the definition of ICT Services now covers almost every aspect of modern value chains, it will increase the efforts to be invested by financial entities and will lead to a high financial impact, leaving financial entities as slow movers and reducing their international competitiveness. To prohibit ICT third party service providers the use of subcontractors is not a viable alternative.

We propose to limit the due diligence obligations to ICT third-party service providers and subcontractors proportionately to those providing ICT services. The disruption would impair the security or the continuity of the service provision. We suggest removing the due diligence requirement completely where the ICT third party service providers prove to have an effective system for vetting and monitoring subcontractors.

Secondly, Article 3(c) requires in most cases that the third-party service provider providing ICT services supporting critical functions must disclose its contracts with all its sub-contractors. This will imply a breach of confidentiality obligations by the ICT third party service provider which are market standard in any ICT service agreement.

Existing regulation requires the outsourcing regulated entity to contractually oblige the insourcer of critical functions to have its contracts with its subcontractors in line with the primary outsourcing agreement, which avoids pre-contractual disclosures of subcontractor arrangements and thus breaches of market standard confidentiality obligations. We propose to use this approach also for DORA.

The term "replicated" implies that the clauses of the primary ICT services agreement must be taken over into the subcontracting arrangements without any textual deviation on a 1:1 basis. This will not be possible in agreements with providers that already subcontracted certain services or with providers that provide services to several financial entities.

The meaning of "as appropriate" following the term "replicated" is unclear as it could either refer to the choice of relevant clauses, the requirement to "replicate" the clauses, or to soften the term "replicated". We propose to use wording that clearly implies that the subcontracting arrangement should be in line with the relevant clauses of the primary ICT service agreement and avoids the interpretation of "replicated".

Thirdly, in Article 3 1) f), the reference to step-in-rights is unclear. Step-in rights are a drastic measure with far-reaching consequences for the ICT third party suppliers subcontracting chain and strong operational effects for the ICT third party service provider.

If DORA is meant to introduce an obligation to implement step-in-rights, it should be made explicit in a separate subclause. This is, however, not feasible.

Generally, we suggest allowing for a proportionate approach to groups. For example, when the subcontractor belongs to the Financial Entity Group a simplified Risk assessment under Article 3 should be sufficient. We also believe that the risk assessment when activities are outsourced to affiliates belonging to the same group of entities should be less cumbersome. For instance, differentiated requirements should apply to affiliates that already have internal knowledge.

Finally, it is not clear how are the requirements listed under Article 3(1) to be complied with or what verification/supporting documents are to be obtained from the third-party service provider.

Please, find below additional specific comments.

Article 3 (1) b):

- It is unlikely that ICT service providers will be willing to accept the involvement of the financial entity.
- It is unrealistic for ICT service providers to inform and involve all financial entities during the decision-making process.

Article 3 (1) c):

- Replication goes far beyond the current requirements. The requirements and the level of details should not exceed the EBA requirements.
- A replication will only be possible if the authority publishes binding standard clauses.

Article 3 (1) d):

- It will hardly be possible to set up the required structure, especially for small ICT providers.
- A financial entity can only have an outside-in view on the ICT service provider's abilities.

Article 3 (1) e):

- It is unlikely to monitor and oversee the subcontractor directly as no direct contractual agreement is in place with the subcontractor.

Article 3 (1) f):

- The information shared by the ICT service providers will not be extensive enough to carry out an adequate assessment on the financial entity's digital operational resilience.

Article 3 (1) i):

- The annotation 'any' is too broad.

Q3: Is article 4 appropriate and sufficiently clear?

No, please consider that the financial entity has no contractual relationship of its own with the sub-outsourcing company. For this reason, the financial entity cannot directly influence the sub-outsourcing company.

Furthermore, the financial entity does not know the contract between the outsourcing company and the sub-outsourcing company and cannot shape it. It can only contractually require the outsourcing company to enter into agreements with the sub-outsourcing company that serve to ensure compliance with regulatory requirements. The financial entity can only exert influence in the contractual relationship with the outsourcing company directly.

The initiative for further outsourcing does not come from the financial entity, but from the outsourcing company.

The requirement of Article 4 to describe in the written contractual arrangements which ICT services support critical or important functions and which are eligible for subcontracting including the respective preconditions may work for classic outsourcing arrangements. However, where ubiquitary cloud services are contracted, market standard agreements are frameworks that allow the use of a broad scale of cloud services, e.g. different compute instance types, storage instance types, specific software etc. These agreements are of general, framework-like architecture and are not specific to certain functions of the financial entity. Such market standard agreements provide the financial entity with the ability to use or refrain from the use of certain or all cloud services. Thus,

the requirement of specific identification of the respective ICT services provided under such agreement as supporting critical or important functions appears to be unrealistic.

Article 4 a):

- It is difficult to agree on monitoring for all subcontracted ICT services. The experience showed that it is even difficult to monitor the first level of subcontracting. Especially in case of multi-tenant service providers, this is not feasible.

Article 4 c):

- It is in general not possible to assess all risks.
- ICT service providers using subsidiaries as subcontractors will not be willing to disclose all risks and to report them to the financial entity (conflicting interests)

Article 4 e):

- Please refer to the comment on Article 4 a). This kind of specification will hardly be possible over the outsourcing chain as no direct contractual relationship between the financial entity and the subcontractor exists.
- Could an annotation 'if possible' be added as this requirement is placed on the ICT service provider?

Article 4 (f) requires a "continuous provision of the ICT services" which implies an availability service level of 100 percent, which is not offered by any ICT provider. Article 4 (f) should rather be referencing the service levels agreed between the financial entity and the ICT third party service provider, e.g. "that the ICT third party service provided is required to ensure the provision of the ICT services supporting critical or important functions in line with the service levels it agreed with the financial entity, even in case of failure (…)".

Regarding Article 4 f) it is not clear how an ICT service provider can provide the service if, for example, a critical ICT sub-service provider fails. It would instead be better to formulate that emergency plans must be available for critical ICT sub-service providers.

Article 4 (g) stipulates that the agreement between the financial entity and the ICT third party service provider shall specify the service levels that each and any ICT subcontractor in the subcontracting chain shall meet. Given the complexity of subcontracting chains in the ICT industry, a financial entity will not be able to fulfil this requirement without suffering an unproportional burden. It should be sufficient, that the ICT third party service provider is obliged and fulfils the service levels promised to the financial entity.

Q4: Is article 5 appropriate and sufficiently clear?

We consider the requirements as clear but not appropriate. Article 5 2) stipulates that the financial entity shall monitor the ICT subcontracting chain inter alia by reviewing the contractual documentation between ICT third party service provider and subcontractors to determine if all conditions referred to in Article 4 are fulfilled.

Given the breadth of what's considered ICT services, the complex ICT subcontracting chains, different jurisdictions to which the subcontracting agreements may be subjected and the cost for legal experts in such jurisdictions to review such agreements, this obligation appears to be overly burdensome without having a proportionate effect on the resilience of the financial entity. It should rather be sufficient to oblige the financial entity to implement an obligation in its ICT third-party service agreements requiring the ICT third-party service provider to establish provisions in its agreement with its subcontractors that are in line with the primary ICT third-party service agreement with the financial entity.

The financial entity should not be required to monitor key performance indicators of its ICT third party service provider's subcontractors. Given the complex outsourcing chains and the number of ICT service subcontracting agreements and subcontractors which may be involved in the provision of the ICT services, this implies a massive effort, which is not proportionate to the effect that may be derived from that monitoring. Monitoring the reported KPIs and reviewing the contract between the ICT service provider and ICT sub-service provider for critical functions represents a considerable additional burden without any clear added value. The ICT service provider is already obliged by the contractual requirements to monitor the critical subcontractor. Furthermore, this requirement is not directly evident in Article 28 (3) and (9) of Regulation (EU) 2022/2554.

Article 5 (1): The requirement in Article 5 of the RTS to have every contract and the KPIs of the sub-service providers along the chain delivered and checked by the institution does not appear to us to be appropriate for achieving the objectives of the DORA. Cloud services in particular use a large number of service providers; obtaining the KPIs and the contract of each sub-service provider and having them checked again by the institution will probably not be made possible by the service providers and will lead to considerable additional work without a corresponding reduction in risk. Confirmation that the provider has passed on all clauses and regularly reviews the performance should be sufficient here, analogous to the EBA Guidelines on Outsourcing para. 80.

Article 5 (2):we see challenges with respect to the implementation of Article 5(2) in relation to external ICT providers as it refers to the contractual relationship between the ICT service provider and its subcontractor. This falls under confidential information (access to the contractual documentation between ICT 3rd party providers and subcontractors) and the Financial Entity would be in this case a third party to the relation between the ICT third party and subcontractor. ICT service providers are unlikely to share contractual documents with the financial entity. This requirement might force ICT service providers to break contractual agreements with their service providers by sending contractual documents to other third parties. NDAs of the ICT service provider and their providers might prevent ICT service providers from sharing contractual documents with the financial entity. The article should be deleted or revised to allow alternative measures under the same purpose, which is the monitoring of the subcontracting chain and be aligned with the EBA guidelines in force on Outsourcing that could be applied vis a vis ICT services.

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

We would not assume ICT third-party service providers would change internal business setups once these are decided on and communicated. The RTS suggests a disproportionate level of influence by the FE. We would suggest a more pragmatic approach to suggest introducing termination criteria based on a change of sub-provider.

Article 6 2) constitutes an obligation on the financial entity to inform the ICT third party service provider about its risk assessment results by the end of a notice period. This obligation is not parametrised, i.e. it does not apply only where the risk assessment is negative. It is not clear, how such obligation shall leverage the operational resilience of the financial entity. The financial entities should be able to act in its sole discretion to provide a – potentially confidential – risk assessment to the provider if it opines that this may be beneficial for it.

Article 6 3) refers to 'material changes' which are neither defined under DORA level I, nor on this draft RTS. This may lead to different interpretations of what might be considered a material change and may lead to further discussions with the ICT service provider in case of a decision on early termination under Article 7 (1) (a). Further clarification on the definition of "material changes" would be helpful to allow for consistent application. Furthermore, large ICT service providers are unlikely to implement material changes only

after the approval of the financial entity. Especially in the context that many financial entities, with different risk profiles, will contact the same service provider.

Additionally, Article 6 3) stipulates, that the financial entity shall require that material changes in subcontracting are only made after approval or non-rejection. This has the effect, that the financial entities are obliged to agree on contractual arrangements with the ICT third party service provider establishing an approval/veto right. This will practically not be achievable in most ICT contracting situations. Art 7 1) stipulates a termination right in case of undue implementation of subcontractings. Such termination rights have proven to be agreeable by ICT service providers. Thus, we propose to amend Article 6 section 3) to the effect that it clarifies, that the contractual implementation of termination rights in case of undue ICT subcontracting is sufficient.

It is not clear if Article 7 requires financial entities to implement the respective termination rights in their contractual arrangements with their ICT service providers, or if Article 7 seeks to establish such termination right. If the latter is the case, this may be welcomed by financial entities, however, from a legal perspective, this is a massive interference in the private autonomy, which faces constitutional concerns. Furthermore, we suggest limiting Article 7(a) to critical and important functions, as it refers to all ICT services, which is not feasible.

Article 8 should take into account the date of first applicability of the DORA requirements for financial entities rather than the day of its application. While financial entities should have a right to be informed of material changes in the subcontracting chain, we do not believe it is realistic to expect them to be able to exercise a right of veto over the appointment of a new subcontractor in all but exceptional cases.

To sum up, Articles 6 and 7 are sufficiently clear from our perspective. However, the requirement for financial entities to inform the ICT third-party service provider of its risk assessment results by the end of the notice period, as put forward in Article 6 (2), appears contrary to our views. We believe that this requirement shall only apply if the ICT service provider is required to take actions following the financial entity's risk assessment. Where no risks are detected and no actions are required from the ICT service provider, the requirement to inform the ICT service provider shall not be mandatory as it would only create additional efforts and overhead for financial entities.

5. Consultation Paper on draft Guidelines on oversight cooperation

Q1: For each guideline, do you consider the Guideline to be clear, concise and comprehensible? If your answer is no, please refer to the specific point(s) of the guideline which is/are not sufficiently clear, concise or comprehensible.

Q2: Taking into account the specific scope of these Guidelines, do you consider that these Guidelines cover all the instances where cooperation and information exchange between CAs and the LO is necessary? If your answer is no, please propose additional areas that should be covered.

Q3: Do you consider that the implementation of these Guidelines will contribute to adequate cooperation and information exchange between the ESAs and CAs in the conduct of oversight activities? If your answer is no, please propose an alternative approach how this could be achieved.

Q4: What are your main expectations regarding the impact on financial entities and CTPPs of the application of these Guidelines?

6. Consultation Paper on draft RTS on oversight harmonisation

Q1: Do you agree with the content of information to be provided by ICT third party providers in the application for a voluntary request to be designated as critical? Please, provide comments on information to be added or removed including the rationale (Article 1)

Legal entity identifier (LEI) can provide several advantages for the identification of financial entities and ICT third-party service providers. However, not all third-country ICT providers may possess or provide trading venues with an LEI, requiring a strong consideration of additional criteria, such as Tax ID.

Q2: Is the process to assess the completeness of opt-in application clear and understandable? (Article 2)

Yes, the process is clear and understandable.

Q3: Is the list of information to be provided by critical ICT third-party service providers to the Lead Overseer that is necessary to carry out its duties clear and complete? Please, provide comments on information to be added or removed including the rationale (Article 3)

We consider that the information to be provided by critical ICT TPPs under Article 3 is extensive and not entirely clear.

It is not entirely clear whether there is a difference between the terms "information about CTPSP market share" in Article 3(2)(d) and " estimation of CTPSP market share" in Article 1(1)(e). We suggest clarifying what kind of "information" about CTPSP market share is required in Article 3(2)(d).

Article 3 (2)(f) appears to be a too far-reaching encroachment on the professional freedom of the CTPSP, as no restriction criteria are provided with regard to the meeting minutes to be disclosed. Such meeting minutes may contain sensitive business secrets of the CTPSP.

Additionally, in some jurisdictions such as Sweden, some information may be prohibited from sharing with the ESAs by certain ICT TPPs due to themselves or their customers being subject to the Swedish Protective Security Act (and other national laws with the purpose of protecting national security).

Examples of information that is very sensitive and therefore may be prohibited from sharing include:

- control measures to protect sensitive data,
- access controls,
- encryption practices,
- incident response plans,
- information about the exact location of the data centres and ICT production centres, including a list of all relevant premises and facilities of the critical ICT third-party service provider,
- information about the overall response and recovery framework of the critical ICT third-party service provider, including business continuity plans and related arrangements and procedures, response and recovery plans and related arrangements and procedures, backup policies arrangements and procedures.

We consider that a mechanism on how to deal with such conflicts of laws/exemptions needs to be established.

Q4: Do you agree with the content of Article 4 on remediation plan and progress reports?

Yes, we agree.

Q5: Is the article on the structure and format of information provided by the critical ICT third-party service provider appropriate and structured? (Article 5)

No, the requirement of Article 5(3) is likely to lead to high costs for the CTPSP based in EU countries where English is not an official language, as the internal documents, such as guidelines, policies, statute documents, minutes of meetings, etc., were originally drafted in the official language of the respective EU country.

Q6: Is the information to be provided by the critical ICT third-party service provider to the Lead Overseer complete, appropriate and structured? (Article 6 and Annex I)

Yes, we agree with the requirements.

Q7: Is Article 7 on competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer clear?

Yes, it is clear.

Q8: Do you agree with the impact assessment and the main conclusions stemming from it?

Yes, we agree.