FINANCE LATVIA ASSOCIATION

Roberta Hirša iela 1, Rīga, LV-1045
Reg. Nr. 40008002175
Phone: 28718175
info@financelatvia.eu
www.financelatvia.eu

RIGA

March 4, 2024
No. 1-27/21

**The European Banking Authority**
*Submitted via the EUSurvey platform*

Re: ESAs Joint Committee second consultation
on Technical Standards under DORA

Finance Latvia Association serves as the representative body for numerous financial institutions, including credit institutions, all of which fall under the scope of regulated entities according to the Digital Operational Resilience Act (DORA) regulation.

In light of the commencement of a public consultation initiated by the European Supervisory Authorities, which consist of EBA, EIOPA, and ESMA and are collectively known as the ESAs, regarding the second batch of policy proposals linked to the Digital Operational Resilience Act (DORA), encompassing four draft regulatory technical standards (RTS), one set of draft implementing technical standards (ITS) and two sets of guidelines (GL), the Association is providing its responses in accordance with the consultation questionnaire.

**Attachments:**

[1.] Response in accordance with the consultation on draft RTSs on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and draft ITSs on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat questionnaire (2 pages);
[2.] Response in accordance with the consultation on draft RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554 (2 pages);
[3.] Response in accordance with the consultation on draft Regulatory Technical Standards specifying elements related to threat led penetration tests (3 pages);
[4.] Response in accordance with the consultation on draft paper on Joint Guidelines on the estimation of aggregate annual costs and losses caused by major ICT-incidents questionnaire (1 page).

Respectfully

Jānis Brazovskis
Board member of the Management Board

Prepared by:
Armands Onzuls, armands.onzuls@financelatvia.eu

**Response in accordance with the consultation on draft RTSs on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and draft ITSs on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat questionnaire.**

**Question 1:** Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

**Answer:** We do not agree with the following requirement due to risk of overreporting:
*According to Dora Art. 19.4 (b) major incidents should be reported '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 are FIs required to send an intermediate report. Additionally, intermediate report requires a lot information to be reported.

**Question 2:** 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.

**Answer:** The reporting item under Article 3 paragraph "g" requires that financial entities have an opinion on the possible impact of an incident on other financial entities and third-party providers. We are not in favour of this requirement since it would force financial entities to make guesses on the possible impact on other firms and their incident response measures. We suggest that the ESAs remove these requirements from the RTS.

**Question 3:** 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.

**Answer:** Regarding Article 4 paragraph "k", information on vulnerabilities exploited could potentially be very sensitive information that FEs would not like to communicate through incident reporting. This kind of information should be communicated through other agreed and predetermined secure channels or even only at physical meetings.

Needed clarification on criteria: *"Information on the impact or potential impact on other financial entities and/or third party providers"*. What FE considers as impact on third party providers on FE incidents, as FE uses other third parties to provide service? Not clear what is meant as third party. Are the "third-party providers" meant that the services are provided to us. Or can it be vice versa (we are the service provider). If yes, do we need to list affected service recipients under "third-party providers" fields? Also, Data field speaks about third party providers, but description on third parties in general. Please, provide instructions on how to indicate third parties. Which one is the case?

Needed clarification on criteria: *"Indication on communication to clients and/or financial counterparts"*. What is meant by "financial counterparts"?

**Question 4:** 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.

**Answer:** Regarding Article 5d) and the field 4.8 entitled *"Date and time when the incident was resolved and the root cause addressed"* in the section on 'Final report' in annex (page 77) it should be clarified which date is to be reported as the date and time when the incident was resolved and the date and time when the root cause was addressed may differ (can be two different dates).

Needed clarification on criteria: *"Information on the impact or potential impact on other financial entities and/or third party providers"*. What FE considers as impact on third party providers on FE incidents, as FE uses other third parties to provide service? Not clear what is meant as third party. Are the "third-party providers" meant that the services are provided to us. Or can it be vice versa (we are the service provider). If yes, do we need to list affected service recipients under "third-party providers" fields? Also, Data field speaks about third party providers, but description on third parties in general. Please, provide instructions on how to indicate third parties. Which one is the case?

Suggestion to change wording in 4.5. "*Information on whether or not and, if so, how contractual arrangements and service level agreements with financial counterparts have been breached or are likely to be breached leading to non-compliance with contractual obligations as a result of the major incident."* as this case does not lead to **non-compliance**, but rather breach of contract.

**Question 5:** 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.

**Answer:** Agree.

**Question 6:** Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

**Answer:** Regarding Article 4, paragraph 1: what constitutes a "secure channel"? What are the requirements? In our opinion, it should be the responsibility of the competent authorities to establish, implement and maintain secure reporting channels that financial entities are comfortable to use, given the sensitive nature of the contents of the incident reporting.

**Response in accordance with the consultation on draft RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554.**

**Question 1:** Are articles 1 and 2 appropriate and sufficiently clear?

**Answer:** While Articles 1 and 2 are appropriate in their scope for the contractual arrangements between financial entities and ICT third-party service providers, we have concerns whether the offered timeline is appropriate for implementation of these requirements for applying them to the already existing, valid arrangements. The list of the risk elements, that should be considered, is quite extensive and our proposal would be to define additional time period, preferably one year after DORA entering into the force, for the existing arrangements compliance with the defined risk management requirements.

In addition, in Article 1(b) it is not clear how the "number of ICT subcontractors" should be considered as an element of increased or reduced risk. For example, is a single subcontractor an increased or reduced risk compared to many other subcontractors?

- e.g., is a single subcontractor an increased or reduced risk compared to many subcontractors?
- Probably a reduced risk could be found when "right-sizing" the number of subcontractors, but how to express that in a usable way in this document?
- Also, there is a difference in risk regarding the number of subcontractors in the ICT subcontracting chain. E.g., even with same number of subcontractors then more breadth in the ICT subcontracting chain could reduce risk (replaceability) but more depth in the ICT subcontracting chain could increase risk (lack of transparency and chained dependencies).

Article 1: Missing the element of "subcontractor maturity" as an element of increased or reduced risk. Subcontractor maturity could be expected to be indicated by e.g., standards certifications (ISO 9000 or ISO 27000 management systems, SOC2 or other) or other ways of proven compliance requiring higher level of maturity (and by that reduced risk).

**Question 2:** Is article 3 appropriate and sufficiently clear?

**Answer:** While article 3 is appropriate in its scope for the contractual arrangements between financial entities and ICT third-party service providers, and sufficiently clear, we have concerns whether an offered timeline is appropriate for applying them to the existing, valid ICT service arrangements supporting critical or important functions. The list of the assessments for subcontractors is very extensive, therefore, our proposal would be to define additional time period, preferably one year after DORA entering into the force, for the existing arrangements compliance with the defined assessments of subcontractors.

Also, regarding section 1. f): The last part of the sentence – "including step-in rights", is not sufficiently clear in this context. Is the intention to clarify that the assessment of the potential impact, should take potentially "step-in" rights" into account?

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

**Answer:** Article 4 is appropriate and sufficiently clear. However, our financial entity has concerns whether an offered timeline is appropriate for applying these RTS requirements towards the contracts, as well as other additional contractual requirements to the existing, valid ICT service arrangements. Taking into consideration the amount of the existing, valid ICT service arrangements, as well as the time required for the negotiations and signing procedure, our proposal would be to define additional time period, preferably one year after DORA entering into the force, for the existing arrangements compliance with the defined contractual requirements.

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

**Answer:** The requirement to fully monitor the ICT subcontracting chain, does not allow for a proportional implementation, i.e. it does not take into account that a) parts of the supply chain would not be directly impacting the services towards the financial entity, and b) the inherent complexity of the supply chain particularly in relation to Software Products.

Article 5(1): It is unclear how far the “fully monitor the ICT subcontracting chain” requirements should go in this chain. ITS Annex 4 "List of ICT services". Is it e.g., only as far as it is pure ICT services being subcontracted (stopping when the subcontracting is concerning other services than ICT like e.g., power, location, manual resources, licences etc.)?

Article 5(2): it is unclear how to monitor contractual arrangements between ICT third-party and their subcontractors. In many case that could be internal, possibly confidential information.

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

**Answer:** The explicit requirement to have contractual arrangements with suppliers supporting critical functions, that would allow the Financial Entity to veto material changes to the supply chain of the supplier, is practically inappropriate for Software suppliers, unless under the oversight of the regulator (Critical ICT third-party service providers), as these suppliers would not be mandated to accept such conditions, which could be materially impacting them in executing their business.

**Response in accordance with the consultation on draft Regulatory Technical Standards specifying elements related to threat led penetration tests.**

**Question 1:** Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed.

**Answer:** Agree.

**Question 2:** Do you agree with this approach? If not, please provide detailed justifications and alternative wording as needed.

**Answer:** The notion of "ICT maturity" is confusing the in the TLPT context. It should be clarified since it could potentially mean a number of different things; How digitalized the financial entity is in terms of business functions and customer services offerings that have a critical dependency on ICT services, or how mature the ICT risk management practices are. In any case, the RTS lacks guidance on how to measure "ICT maturity".

**Question 3:** 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.

**Answer:** Article 2, paragraph 3: in this paragraph, the discretion to interpret and set scales and threshold for various criteria are left to the individual TLPT authorities. We encourage the ESA, for each criteria, to develop clear scales and thresholds to include in the RTS.

**Question 4:** 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.

**Answer:** No. More detailed explanation on criteria "Where more than one financial entity belonging to the same group and using common ICT systems or the same ICT intra-group service provider" would be needed. e.g. if entity belonging to the same group but using separate instance of the same ICT system qualifies as criteria not to perform the TLPT for that entity. How significant differences in ICT systems will be considered as not eligible for not to performing separate TLPT.

It is not clear how TLPT authority(ies) of the Member State(s) will coordinate inclusion of group entities operating in different countries into scope of TLPT.

**Question 5:** Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions.

**Answer:** Yes, the Generic Threat Landscape from TIBER could be a construct that would benefit the participants to share cost and an aligned view on the generic threat landscape. Also, the concept of Key systems with the scope definition allows for focusing on the most important systems, in contrast with Annex II.2.b.ii, which suggests systems supporting, which could mean a lot more systems.

**Question 6:** 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.

**Answer:** In Article 5.2.g it is difficult to understand what kind of "restorations" threat intelligence providers must do.

**Question 7:** 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.

**Answer:** No. Availability of qualified external testers and threat intelligence providers is unclear/questionable. Is there any valid market research regarding availability of external testers that corresponds to the requirements specified.

ESAs should consider a central EU certification program, if they want to ensure quality alignment between all entities or use a similar approach like in the UK CBEST framework where there are clear indicators, which certifications are required for both the intelligence provider and the testers. Alternatively, and Hong Kong iCAST-approach could also be used, that allow organization to define certifications and equivalents and agree this with the competent authority.

**Question 8:** 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.

**Answer:** No. Number of years of experience will not be appropriate measure. Quality and testing coordination procedures within test provider are more important. Availability of qualified external testers and threat intelligence providers is unclear/questionable.

Instead of the number of years of experience, the amount of previously finalized TLPT/TIBER-like projects plus certifications, would be a better measure. If the ESAs wish to impose this level of assurance on the testers, they should be very specific on requirements, make the requirements meaningful (number of years of experience says nothing about the skill level). A centralized accreditation system would be appropriate.

Is there any valid market research regarding the availability of external testers that corresponds to the requirements specified.

**Question 9:** Do you consider the proposed process appropriate? If not, please provide detailed justifications and alternative wording as needed.

**Answer:** Regarding Article 8, paragraph 5: we object towards setting a minimum time limit as a way to define the effort and complexity of the test. The length of the test says nothing about the quality. As an example, an experienced, but unskilled tester can spend 12 weeks not finding any relevant vulnerabilities that a skilled freshman will exploit in a few days. We suggest that the time limit should be defined by the financial entity and approved by the TLPT authority before the testing to ensure an adequate level of the testing to be performed.

Additionally, strict timing between phases (e.g. within 4 weeks) may be difficult to fulfil, if e.g. a test is delayed, and the period falls into the vacation period. Also, length of testing phases must be shorter to reduce overall cost of TLPT and guarantee availability of testers.

**Question 10:** Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.

**Answer:** The risk that the same organization may get tested several times depending on the Member State authority that leads the testing and what it decides on should be avoided.

**Question 11:** Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.

**Answer:** We see a benefit in using both internal and external testers, therefore use of internal testers must be allowed. Availability of qualified external testers and threat intelligence providers is unclear/questionable.

The definition of external tester is not clear, e.g. are testers from another legal entity belonging to the Group of entities are considered external?

**Question 12:** Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.

**Answer:** Most likely that will require a lot of work and coordination among the supervisory authorities and will take some time until the mechanism works well, therefore the RTS should clearly specify which supervisory authority applies as Lead authority and has ultimate responsibility to coordinate the TLPT process. It is not clear how this cooperation will be performed in case of significant financial entities in various member States reporting to ECB but belonging to Group.

**Question 13:** 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.

**Answer:** Maintaining TIBER framework and DORA requirements in parallel seems unnecessary and an additional layer of complexity that can be avoided. If DORA is laying out the principles for TLPT to FEs, then it does not make sense to have financial entities regulated by DORA, also be included in the scope for TIBER. Especially as TIBER will be reviewed to comply with DORA requirements. It could just be made redundant for FEs regulated by DORA as this could also be regarded as a proportional application of EU law, which covers a similar or overlapping topic.

**Response in accordance with the consultation on draft paper on Joint Guidelines on the estimation of aggregate annual costs and losses caused by major ICT-incidents questionnaire.**

**Question 1:** 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.

**Answer:** Agree.

**Question 2:** 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.

**Answer:** Agree.

**Question 3:** 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.

**Answer:** Agree.