FINANCE
LATVIA
ASSOCIATION

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

RIGA

August 30, 2023
No. 1-27/88

The European Banking Authority
Submitted via the EUSurvey platform

Re: ESAs Joint Committee 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 recent 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 initial batch of policy proposals linked to the Digital Operational Resilience Act (DORA), encompassing four preliminary regulatory technical standards (RTS) and an initial set of implementing technical standards (ITS), the Association is providing its responses in accordance with the consultation questionnaire.

Attachments:

[1.] Response in accordance with the consultation on draft RTSs ICT risk management tools methods processes and policies questionnaire (6 pages);

[2.] Response in accordance with the consultation on draft RTS on classification of ICT incidents questionnaire (2 pages);

[3.] Response in accordance with the consultation paper on draft ITS on register of information questionnaire (5 pages);

[4.] Response in accordance with the consultation paper on draft RTS on policy on the use of ICT services regarding CI functions questionnaire (3 pages).

Respectfully

Sanita Bajāre
Chairperson of the Management Board

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

Response in accordance with the consultation on draft RTSs ICT risk management tools methods processes and policies questionnaire

Question 1: 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.

Answer: The biggest concern of article 15 and article 29 is timeline of implementation, as is touches a lot of areas where improvements will be needed. It is not realistic to implement all parts of the mentioned elements till 17.01.2025, taking in account that RTS will be approved only next year.

Question 2: 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.

Answer: No response.

Question 3: Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

Answer: In Article 2 – Provisions on Governance, should be adjusted 2nd line responsibilities as in (b) point – 2nd lined does not manages ICT Risk, (c) point – does not defines ICT and information security objectives and in (f) point does not develops ICT security awareness programs.

Question 4: Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.

Answer: Agree.

Question 5: Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.

Answer: We suggest the following changes to Article 5, paragraph 2 to reflect that the risk assessment should not influence or inform the criticality assessment. They are distinctive steps that should be done in sequence:

> *2. Such procedure shall detail the criteria to perform the criticality assessment of information assets and ICT assets supporting business functions. Following the criticality assessment, the ICT asset management procedure shall take into account the ICT risk related to those business functions and their dependencies on the information assets or ICT assets and how the loss of confidentiality, integrity, availability of such information assets and ICT assets would impact their business processes and activities.*

Question 6: 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?

Answer: Yes, agree to keeping record on end date, this is a basic expected control within ICT system lifecycle management.

Question 7: Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

Answer: Encryption of data in use, as mentioned in Article 6 paragraph 2a is an immature technology with large consequences on performance and ICT system design with limited use cases. It is further unclear what additional controls "separated and protected environment" entails when encryption in use is not possible, as separated, and protected environments is already described elsewhere.

We suggest the ESAs to reverse the requirement and state that in situations where separation and protection cannot be achieved by other means, encryption in use can be used to mitigate such separation and protection. We suggest the following wording of Article 6 paragraph 2a:

> *2. The policy on encryption and cryptographic controls shall include all the following elements:*
> *(a) rules for the encryption of data at rest, in transit and, where relevant, in use, taking into account the results of the approved data classification and ICT risk assessment processes to protect the availability, authenticity, integrity and confidentiality of data.*

Question 8: 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.

Answer: A separate and protected environment can also be used to ensure the confidentiality, integrity, and availability of data. In situations where separation and protection cannot be achieved by other means, encryption-in-use technologies can be used to mitigate such separation and protection requirements.

Question 9: Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

Answer:

- Article 8, paragraph 2b, ii: We suggest that the ESAs clarify 'scheduling'. Does it for example refer to batch jobs, scripts, or backups? If the ESAs specifically meant to reference backups a reference to Article 8, paragraph 2b, i? If so, a reference to backups is needed.
- Article 8, paragraph 2b, iii: The use of the word 'protocols' could be misleading. We suggest that 'protocols' is replaced by 'requirements' and that 'requirements' then is removed in iv and v.
- Article 11, paragraph 2a: It is not clear what is meant by 'the access restrictions'. This should be clarified by the ESAs.

Question 10: 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.

Answer: No.

Question 11: 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.

Answer: Formulating the requirements as “automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile” would be too comprehensive to be practically achievable for a financial entity considering the full range of ICT assets of different types (e.g. hardware, network configurations, firmware, virtual machines, operating systems, platforms and application), their part and location in the overall architecture (internal vs externally exposed) and also all different types of vulnerability scans that can be applied (e.g., unauthenticated scans like port scanning, and agent based or authenticated scans for details on installed ICT assets). It would create a burden to scan all ICT assets, also it would give a lot alerts, where would be needed additional resources and costs increases. And it would not make sense to make scans to all ICT assets as it does not support the proportionality principle. In essence the statement of “all” should be reformulated to specify a more relevant practical scope, but still covering both higher and lower information classes as commented above.

Question 12: 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**.**

Answer: Agree.

Question 13: Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.

Answer:

- Article 13, paragraph 1b: The visual representation of all the financial entity's data flows is for a larger financial entity unreadable since presenting all data flows in the same visual becomes too cluttered. The ESAs should clarify the objective to be achieved by visualization. This will make it easier for financial entities to construct a visual representation that is fit for purpose.
- Article 13, paragraph 1c: This item is unclear in terms of dedicated network. At what level should networks be dedicated? The items do not consider the different set-ups needed to securely administrate e.g., a network device vs a server farm vs an application on a server vs a cloud application. Also "direct internet access" is not clear as a limited direct internet access to a specific service is tied to much less risk than e.g., internet wide indirect access via a proxy. We suggest that the ESAs re-write this item to focus on the expected outcome for financial entities rather than keeping the current prescriptive requirement on "a separate and dedicated network for the administration of ICT assets…".
- Article 13, paragraph 1l: It is unclear how session management is related to network security. Locking systems or even terminating sessions that are inactive on application layer is primarily the responsibility of an application. The network only has information to act on network traffic patterns (e.g., open connections that are unused). The ESAs should clarify this item.
- Article 13, paragraph 1m: This item is hard to understand in general. As an example, what is meant by "network services agreement"? What parties engage in this agreement? The ESAs should clarify this item.

Question 14: 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.

Answer: No response.

Question 15: Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

Answer:

- Article 15: These requirements could be perceived to dictate that project management and system development methodologies should follow the waterfall model, i.e., a linear sequential design approach for ICT project management. Most financial institutions have already or are in the process to adopt agile software development. This article could limit the options available for financial institutions, in this case not only related to risk management but also to business development. We suggest that the ESAs re-draft this article to cater also for non-project-based ICT-development methodologies.
- Article 16, paragraph 4: The reference to dynamic testing as part of source code review is unclear. Dynamic testing is done on a running system, not on the source code, and would therefore constitute a separate complementary activity to source code review and static testing of code. The ESAs should clarify this item.
- Article 17, paragraph 2: 'systems' are specifically mentioned to be in scope of the ICT change management procedure alongside software, hardware, firmware. To clarify the

paragraph, we argue that 'systems' should be removed since systems are composed of software, hardware, and firmware.

The requirements detailed in Article 16 (ICT systems acquisition, development, and maintenance) does not cater for the real-world duality of an ICT System, being either provided by the ICT organization (as now assumed in Article 16) or developed by the business itself as an EUC - End-user Computing Application (typically not covered by ICT project management). The proposed requirements of this RTS therefore contradicts the existing requirements from EBA/GL/2019/04, where it is stated under chapter 3.6.2 (ICT systems acquisition and development), that: "*74. A financial institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.*".

For these ICT Systems being ICT systems, the requirements stated in Article 16 would not be possible to fulfil (given the nature of an EUC being managed outside the ICT organisation). Still these EUC needs to be identified and related to critical or important functions, but they cannot practically apply same requirements due to that the business normally lacks dedicated testing environments nor technical tools or competences for code review, nor formal ICT project management competences.

Please note: Trying to apply too strict requirements on EUC ICT systems will not improve them but rather turn them into "shadow ICT" where they are not identified nor documented as connected to critical or important functions. The key is to find a practical balance and a risk-based approach between centrally managed ICT and End User Computing.

Question 16: 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.

Answer: No response.

Question 17: Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.

Answer: No response.

Question 18: Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

Answer: Article 18, paragraph 2d: 'information processing facilities' should be clarified by the ESAs. It is not used in the corresponding DORA level 1 requirements.

Question 19: Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

Answer: Agree, no additional measures needed.

Question 20: Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

Answer: Disagree. Not all training should be annual, as it would be a burden for organizations. Also, some trainings should be limited to very specific employees – not all personnel.

Question 21: Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.

Answer: Article 22, paragraph 1e, iv: This item mentions 'critical ICT systems'. Should this be interpreted as ICT systems that are supporting critical or important functions? If so, this expression should be used for clarity of the requirement. Open question would it not be a burden that at least every 6 months ICT systems, which are supporting critical or important functions access rights must be reviewed? (Depends also on count of functions x systems).

Question 22: 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.

Answer: No.

Question 23: 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.

Answer:

- Article 23, paragraph 1f: The mentioning of ICT response and recovery plans in this paragraph seems erroneous and should be removed by the ESAs. ICT response and recovery plans requirements are specified in article in Article 27.
- Article 24, paragraph 2b: Is "data sources" referring to data sources for log data or the data sources used by assets supporting critical or important functions? The ESAs should clarify this item.

Question 24: Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

Answer:

- Article 26, paragraph 2c: This is the only paragraph in the RTS that mentions 'critical business functions'. Should it in fact be 'critical or important functions'?
- Article 27, paragraph 1b: items mention 'critical ICT systems and service of the financial entities'. Shouldn't it be 'ITCT systems and services supporting critical or important functions'?

Question 25: Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

Answer: No response.

Question 26: 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.

Answer:

- Article 28, paragraph 2a, ii: Since the ESAs draft the requirements of the RTS, they should also define the purpose of this required report.
- Article 28, paragraph 2h, v: What is meant by 'major and immediate deficiency'? Does it differ from the requirements to report major ICT incidents? The ESAs should clarify this item.
- Article 28, paragraph 2, l: Compliance and risk oversight are two separate functions.

Question 27: Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.

Answer: No response.

Question 28: 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.

Answer: Agree.

Question 29: 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.

Answer: No response.

Question 30: 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.

Answer: No.

Question 31: 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.

Answer: No response.

Question 32: 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.

Answer: No response.

Response in accordance with the consultation on draft RTS on classification of ICT incidents questionnaire

Question 1: 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.

Answer: No, the proposed approach could lead to significant overreporting regarding short term DDOS attacks (e.g. affects critical service + potentially all clients but for couple of minutes). Suggested to include 2 primary and at least one secondary or more simply any 3.
In their efforts to comply with the RTS, it is important for financial entities to be able to clearly determine what parts of their business operations are in scope for ICT related incident classification. Currently, the RTS is using several different terms such as 'the service', 'critical services affected', 'critical functions', 'non-critical services', and 'critical or important functions' that brings unclarity and legal uncertainty for financial entities. We suggest that the ESAs only uses the term 'critical or important functions' throughout the RTS for clarity, since this term is clearly defined in the level 1 text in DORA.

Question 2: 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.

Answer: No, not clear where this information could come from. It requires a lot of effort to make such data in usable format and keep them up to date. Even if this info is collected from the counterparty in contract signing moment, the service relevance to their business might change with a time.

Question 3: 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.

Answer: Regarding 'Reputational impact' criteria b) and d) are agreeable as it uses the plural form of 'complaints', 'clients', and 'counterparts' (not to get overreporting on single cases), and criterion c) is fine as is. However, criterion a) lacks this levelling, and we suggest that there is additional wording added to allow for the distinction from e.g., a single user posting a negative comment in a social media channel vs. a national newspaper posting a negative article. A possible suggestion for wording criterion a) could be "The incident has attracted multiple media attention", to cover the fact that more significant media attention (even if posted only once) will lead to re-posts and remarks in other media, that in total can be expressed as "multiple media attention" – whereas a single post from a single user in e.g. social media stays limited and should not be considered a criterion for a major incident. Concerning Art.7 a clarification on reporting of costs and its purpose is needed (do we only mean material costs?). Clarification needed on what is meant by financial market infrastructure or third party assessment.

Question 4: 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.

Answer: 'Data losses' and proposed criterion 1) (in relation to the availability of data), we propose to clarify that data loss should be assessed versus data is made permanently inaccessible or unusable. The aspect of temporary unavailability is already covered by criteria 1 – 'Clients, financial counterparts and transactions' and should not be duplicated under data loss.

Question 5: 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.

Answer: Currently, the RTS is using several different terms such as 'the service', 'critical services affected', 'critical functions', 'non-critical services', and 'critical or important functions' that brings unclarity and legal uncertainty for financial entities. We suggest that the ESAs only uses the term 'critical or important functions' throughout the RTS for clarity, since this term is clearly defined in the level 1 text in DORA.

Question 6: 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).

Answer: Agree.

Question 7: 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.

Answer: Agree.

Question 8: 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.

Answer: Agree.

Response in accordance with the consultation paper on draft ITS on register of information questionnaire

Question 1: 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?

Answer: Only part of third-party ICT service providers have a LEI code. If LEI code is existing there shouldn't be any obstacles to provide it. But overall, the field shouldn't be mandatory for the cases when the codes are not existing and only company registration code could be provided. Why LEI code should be requested from critical or important ICT providers and sub-contractors?

Question 2: 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?

Answer: No, we do not agree with proposed formulation of Article 4(1)b. This is due to: As the FE only knows of and can control the contractual relations regarding the direct ICT third-party service provider, any material subcontractors can reasonably only extend one step in the value chain of any subcontractor(s), as the statement of "all" might be practically impossible for an FE to ensure (possible in unlimited number of steps).

More detailed explanation is needed for the definition "material subcontractors", since it is not clear if material by the spend (dedicated to subcontractor), material by services provided to the bank, material by subcontractor's size? Or material shall be interpreted as per description: "Material: in case of disruption of the ICT services, the supported functions would be significantly impacted if the disruption lasts more than few minutes/few hours, and the disruption may engender damages, but still manageable"? Once the definition will be clear the requirement to maintain register info on sub-contractors needs to be reassessed.

In addition, if talking about "ICT Service supply chain" – do we need to keep information of such ICT service provider's sub-contractors, if this subcontractor directly is not related to the services that the financial entity is receiving, but its general ICT service provider will not be able to provide service without such sub-contractor. E.g. Bank is subscribing Software solution X (on premise) for one of the critical function execution from ICT provider Y. This ICT provider Y for the implementation of new functionalities and for functions testing are using sub-contractors Z and P. Directly those sub-contractors Z and P are not related to the Bank. Shall we keep information of such sub-contractors?

Question 3: 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.

Answer:

As the template for Contractual Arrangements RT.02.02 implies a duplication of entries based on a broken ICT service taxonomy, the work of decomposing the actual contractual arrangements into both a functional grouping and ICT service taxonomy/categorisation will be cumbersome and not relating to the real contractual situation. There is a significant risk that this reporting will be fictitious and not relevantly reflecting the real situation, and also being hard to maintain and keep correctly updated over time. Any reporting should be close to the real situation and how the third-party contractual arrangements support the (critical or important) functions of the FE.

Tasks:

- Review of all banks agreement to identify ICT arrangements.
- Classify all arrangements in terms of critical or important.
- Development of new registry for ICT arrangements on the internal systems.
- New process setup for different information collection: bank assets and financial indicators, yearly budget and spend info update, etc. As well as rules for spend conversion to EUR (at what time and what exchange rate) should be prepared.
- New processes for reporting on entity and on sub-consolidated and consolidated levels.
- Taxonomy for functions identification shall be created on the group or company level.
- Clear rules for registry updating shall be implemented.
- Amendments to the existing contract templates will be mandatory to implement new requirements for ICT providers and sub-contractors to procure and maintain valid LEI codes.
- Educate the whole organization on the new register and necessary information.
- Collecting data for the registry.

Operational issues:

- At the moment no indicators which data is necessary for Critical / important ICT arrangements only. We assume that there should be more such fields. Otherwise, the scope of the information that should be collected for all ICT arrangements does not seem to be reasonable and risk-based approach is not followed.
- We see significant overlap with outsourcing registry, however it is far an exact match, so perhaps it is reasonable to align all registries.
- Registry of such large scope of data, especially considering the fact that large proportion of info entries are new, will be extremely time consuming to prepare, from process setup to system development, to training, to collection and actual entry of data.

Question 4: 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?

Answer: What are the arguments for reporting contracts that are expired for 5 years? 5 years' time period is very long and within the period enormous amount of contract entries will be recorded, especially if all needs to be kept in the same registry. At some financial entities after contract is expiring / terminated, within the period set in internal instructions, such contract is archived, and upon the need contract data can be retrieved from an archive. In addition, as soon as the contract is terminated / closed there shouldn't be a need to maintain expired contract info if it is no longer in use.

Question 5: Is Article 6 sufficiently clear regarding the assignment of responsibilities for maintaining and updating the register of information at sub-consolidated and consolidated level?

Answer: From article 6 it is clear that 3 levels of registers shall be maintained: entity level, sub-consolidated and consolidated. The ultimate parent undertaking shall define the scope of consolidation. Other than that, responsibilities for maintaining and updating are not clear and not defined. What's the need to have separate consolidated registry on a group level, if all group legal entities shall have and maintain their separate registries? This requires double or triple manual work to maintain contract information in 3 registries. It would be less complicated to have additional identifier for group related agreements (in the same one registry), and once it's needed to have consolidated view all related agreements would be marked. In addition, how far consolidation requirements shall be applicable to other group entities, that are not banks, e.g. Leasing companies?

Question 6: 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?

Answer: Consolidated level registry may be maintained and updated only by the ultimate parent company, which is Skandinaviska Enskilda Banken AB (publ). Therefore, entity level and, when applicable, sub-consolidated level registries may be fully maintained by each SEB bank in the Baltics.

Question 7: 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?

Answer: Depending on the logic of the questions provided in each template would be preferable finding budget and spend questions in the template: "Contractual arrangements – Specific information". Budget and spend data is on the same level as contract start and end dates, termination period and other information that is requested in Specific information category. In addition, the past year value is largely understandable, however, upcoming year cost may be problematic to provide accurately as some agreements are dependent on use cases. Perhaps keeping just, the past year value would be the most accurate.

Question 8: 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?

Answer: No, we do not believe the proposal capture the full or correct ICT value chain. This is due to:

- The ICT service identification is not a proper taxonomy, but rather a categorisation.
- The ICT value chain should be based on the actual contractual relationship and the actual IT services provided (with applied ICT service categorisation). The FE should identify each ICT service provided by the ICT third-party by an unique service id (unique for each FE), and then apply a service categorisation (one or many) to the actual ICT service provided.

Current explanation for the "RT.05.02.0060 Rank" field indicates indefinite list of ranking of sub-contractors. Depending on the full definition of "material sub-contractors" (in case it is broad), perhaps a limit to the rank may be introduced as per proportionality principle. Alternatively, if the definition would be rather precise, that would, by default, limit the potential ranking. In general, it is not clear how to fill in template RT.05.02 questions, therefore detailed example would be needed. For example: Company X has a contract with company A to receive company B's services. A and B have a contract. X and B do not. Additionally, B further contract company C to fulfill obligations to A (and, therefore, X). In such a case, B is the ICT third-party service provider (RT.05.02.0030-50), Rank 2, and the recipient of sub-contracted ICT services (RT.05.02.0070-90) is A. Also, C is the ICT third-party service provider (RT.05.02.0030-50), Rank 3, and the recipient of sub-contracted ICT services (RT.05.02.0070-90) is B. Is that the correct manner of filling this part of the RT.05.02 template? Also, should rank 1 with A and X be entered?

Question 9: Do you support the proposed taxonomy for ICT services in Annex IV? If not, please explain and provide alternative suggestions, if available?

Answer: No, we do not believe the proposed taxonomy is useful. This is due to:

- As a taxonomy it should support classification of services that is mutually exclusive and non-overlapping. The proposed set S1 to S20 do not meet these criteria (e.g., S9 vs S18/19 or S7 vs S19/S20 etc.) and opening up for further classes (S21->) will probably complicate this even more.
- As best this can be used as an ICT Service categorization, i.e., a grouping based on perceived similarity and possibility to tag is any number of relevant service categories, and not as a taxonomy.
- Also, the name of RT.07.01 "ICT service identification" is misleading as it is not about identification of ICT services, but categorization of ICT services.

Additionally:

- S1 – What type of ICT service should be applicable in terms of permanent license? What type of ICT services should be applicable if software is purchased as an asset and contract is for maintenance and support?
- S2 and S3 – as per description overlaps, OR there should be provided more detail explanation what development is covered under S2 and S3.
- S4 – what about ICT change management services? Does it cover?
- S8 - Rental of facilities and physical infrastructures – does it mean that all Data center premises rental agreement shall be classified as ICT arrangement? What does is it mean – "provision of fluids". What scope of physical onsite security S8 shall cover (e.g. office / branch onsite physical security)? Shall S8 also cover electricity or any other utility services?
- In case of telecom services how to differentiate S8 and S11?
- In case of Full Time Consultants (FTC) procured for e.g. analysis and development of requirements (for reporting, for software implementation) shall it be treated as S3 or S16?

Question 10: 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?

Answer: What kind of total assets shall be reported? What is reasoning behind of collection of such information?

Question 11: Is the structure of the Register of Information clear? If not, please explain what aspects are unclear and suggest any alternatives, if available?

Answer: No, we do not believe the structure is clear or useful. See answers to questions 2, 3, 8, and 9. Structure of the registry is understandable; however, the amount of overlapping information complicates and confuses a lot. Perhaps one 'key' per sheet could be sufficient.

Question 12: 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?

Answer: No, we do not agree on the level of information. This is due to:

- Proposed ICT service taxonomy is not a taxonomy, but at best a categorisation.
- The actual ICT services used by FE is not identified (using FE's identities, i.e., "service ids").
- The scope of "all the material subcontractors" is not limited enough (see question 2 above).

To fulfill the three purposes of the Register of Information, the level of information is sufficient. Perhaps for non-C/I case full scope of information is less so necessary as per the proportionality principle. In other words, we see value in introducing column asking weather arrangement is C/I or not, then enabling a decreased number of mandatory fields for non-C/I ICT arrangements, in particular, template "R08.01: Assessment of the ICT services" could be applicable only to C/I. Additionally, it is already so in the case of Outsourcing reporting requirements. In addition, cloud-related arrangements reporting is not covered in the registry.

Question 13: 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.

Answer: No response.

Question 14: Do you agree with the impact assessment and the main conclusions stemming from it?

Answer:

- POLICY ISSUE 6: USE OF THE LEI CODE TO IDENTIFY ICT THIRD-PARTY SERVICE PROVIDERS – we see the risk that such requirement may limit our selection of ICT 3rd party providers in the market, since we may struggle to convince 3rd party providers to purchase and maintain LEI codes only for our service provision, since having a LEI code for ICT 3rd party provider doesn't provide any additional value. Suggestion would be not to limit only to LEI codes, but to consider using country registration codes for reference.
- POLICY ISSUE 7: DETAIL OF INFORMATION REQUIRED IN THE REGISTER OF INFORMATION – we haven't found any indication on Due Diligence or risk assessment in the template for fields mandatory only for C/I.
- POLICY ISSUE 8: ICT SERVICE SUPPLY CHAIN – we haven't found any indication on Due Diligence or risk assessment in the template for fields mandatory only for C/I.
- POLICY ISSUE 9: TAXONOMY FOR FUNCTIONS – suggestion would be to reassess the decision of creation universal function taxonomy since it might be reused from other sources. Especially since the review is likely anyway, the need to create separate taxonomies for each legal entity is seen more as introduction of more chaotic approach, decrease in alignment across different entities, potential mistakes due to mismatches. We encourage you to review existing other taxonomies from other FEs and / or any potential learnings from Outsourcing area.
- POLICY ISSUE 11: RECORDING OF TERMINATED CONTRACTUAL ARRANGEMENTS – more arguments are needed why 5 years period for contract information keeping were selected. Does it mean that contracts that are expired for up to 5 years shall be also reported and information shall be maintained and updated after the termination?

Response in accordance with the consultation paper on draft RTS on policy on the use of ICT services regarding CI functions questionnaire

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

Answer: General comment: There are several regulations (DORA, EBA Guidelines on outsourcing arrangements, normative acts related to the transposition of Directive 2014/59) that cover requirements for different types of Third-Party Arrangements (mandatory clauses in the agreement, registry requirements, due diligence etc.). Suggestion to align the regulatory requirements, incl. further regular reporting to supervisors.

- Proportionality principle applicable for the policy on the use of ICT service supporting C/I functions shall focus on the elements of increased complexity or risk, i.e. vendors providing services or their parent companies from outside EU/EEA, in case vendor is processing high sensitivity class data and in case data is stored / processed outside EU/EEA. It seems to be appropriate and sufficiently clear. Nevertheless, when looking into draft 03 ITS on register of information there are no indication that C/I ICT suppliers shall be treated differently, and distinct level of information shall be logged and maintained for both categories C/I and non-C/I. Therefore, a level of clarity in terms of policy vs. registry alignment would be appreciated.
- It should be clarified - how far the responsibilities apply to subsidiaries that are not considered as financial entities (like Leasing company)?
- EBA Guidelines on outsourcing arrangements require to have Outsourcing policy. It should be clarified how DORA and outsourcing requirement must be linked. Is it expected for the financial entities to have 2 independent policies or can both regulatory requirements be covered by one policy?

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

Answer: Some questions that should be clarified:

- Is the mentioned financial entity's audit plan understood as financial entity's Internal Audit plan or separate audit plan is expected for Third Party Arrangements?
- It should be clarified if the financial entity when executing this audit plan should perform audits on the ICT third party service provider on behalf of the financial entity's management or if the audit should assess the financial entity's oversight and risk management over the ICT third party or both.
- It should be clarified if the financial entity should perform audit on ICT third party service provider for critical or important function annually or the frequency could be subject to risk-based approach (our suggestion is to keep as risk based approach).
- The term 'member of senior management' should be clarified by the ESAs. Should this in all cases be an individual reporting directly to the CEO of the financial entity?
- Article 3, paragraph 8: This paragraph requires that the CI services in scope that are provided by ICT third party service providers are included in the financial entities audit plan. However, it should be clarified by the ESAs in this paragraph if the financial entity when executing this audit plan should perform audits on the ICT third party service provider on behalf of the financial entity's management or if the audit should assess the financial entity's oversight and risk management over the ICT third party or both.

Question 3: Is article 4 appropriate and sufficiently clear?

Answer: Overall Article 4 is clear, nevertheless the differentiating factors that shall be applicable to the policy cannot be identified in the 03 ITS on register of information. If the policy shall differentiate providers between: (a) registered in MS and under DORA regulation vs. not; (b) intra group vs external; (c) located in MS vs located in third countries; then the same differentiation shall be possible in the register of information. More detailed guidelines for differentiating suggested three types of ICT service providers shall be provided. It should be specified up to what level of contracting should be included when applying requirements to subcontractors.

Question 4: Is article 5 appropriate and sufficiently clear?

Answer: Article 5, paragraph 1f: The term 'the involvement of business units' should be clarified by the ESAs. What are the responsibilities that the RTS is placing on the financial entities business units? Article 5, paragraph 1f: It is unclear what is meant by 'internal controls' in this paragraph. Are the ESAs referring to a specific function in the 2nd line of defense or 1st line of defense?

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

Answer: Some questions that should be clarified.

- It is not clear to what extent subcontractors should be covered by this Ex-ante risk assessment.
- Regarding Due diligence section: "(b) uses or intends to use ICT sub-contractors to perform material part of their services", it should be clarified how "material part" should be measured.
- Article 7, paragraph 1a: The paragraph is referring to 'appropriate organisational structure, including risk management and internal controls…'. However, risk management and internal controls are not organisational units in a financial entity but rather risk management concepts. The ESAs should clearly specify what function are in scope, using more precise language such as ' the risk management function in the 1st line of defence' as an example.
- Article 7, paragraph 1a: The paragraph requires that ICT third party services providers in scope should 'have an effective and sound digital operational resilience framework'. The ESAs should clarify what is meant by 'effective' so that financial entities can determine what actions to take in its due diligence procedures. In addition, this requirement is not consistent with Article 7, paragraph 2 that requires that the policy shall '…specify the required level of assurance concerning the effectiveness of ICT third-party service providers' risk management framework for the ICT services to be provided by ICT third-party providers to support critical or important functions. We propose that the ESAs remove the parts from Article 7, paragraph 1a that requires 'effective and sound digital operational resilience framework'.

Question 6: Is article 8 appropriate and sufficiently clear?

Answer: Article 8, paragraph 1: To clarify what financial entities should achieve by identifying conflicts of interests, the ESAs should specify the purpose of this activity. What types of conflicts of interest should be identified?

Question 7: Is article 9 appropriate and sufficiently clear?

Answer: It should be clarified how these requirements should be linked and aligned with outsourcing and recovery planning requirements (please see also General comment in 1st Answer). Also:

- Article 9, paragraph 2 and 2b: The ESAs should clarify what is meant by 'ICT testing'.
- Article 9, paragraph 3: The ESAs should clarify what is meant by requirement third-party certifications and reports as referred to in paragraph 2 (c) are adequate and sufficient to comply with their regulatory obligations and shall not rely solely on these reports over time.

Question 8: Is article 10 appropriate and sufficiently clear?

Answer: Some clarifications are needed:

- Article 10, paragraph 1: The paragraph requires financial entities to 'monitor, on an ongoing basis, the performance of ICT third party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information'. It should be clarified by the ESAs what these requirements originates from. Is it DORA requirements or the financial entities own requirements (that could, among other frameworks and the financial entity’s own risk assessment, be based on DORA)?
- Article 10, paragraph 2b and 2e: These items could be combined by the ESAs since they both require independent reviews.
- Regarding cloud service providers it is not possible to fulfil these requirements on contractual arrangement level as they reside on service functional level and are subject to customer configuration. It should also be noted that financial institutions do not have an equal bargaining power when negotiating contractual terms with CSPs; it is not possible to change the standard cloud service provider agreements. Standard EU contractual terms for cloud services would be highly welcomed.

Question 9: Is article 11 appropriate and sufficiently clear?

Answer: There is need for clarification what is meant by exit plan testing. It would be more appropriate to perform tabletop exercises to validate the exit plan. Also, it is not clear what the requirements regarding the timeframe for exit plan are under this Article (should it be 1, 6, 12 or 24 months). Intra-group ICT service providers shall be excluded from the requirements of this article.