Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA RTS on ICT risk management framework and RTS on simplified ICT risk management framework

Date: 18 August 2023
EU Transparency register: 3505006282-58

General Drafting Principles
Q1. Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (Complexity and risks considerations)? If not, please provide detailed justifications and alternative wording as needed.
No While it is essential to incorporate proportionality in the RTS based on Article 15 of DORA, it is not possible to observe the proportionality principle being applied consistently on the entire RTS. Notably, when it comes to the frequency of certain controls, especially under Section V ICT Operations Security and Section VI Network Security, the prescriptive type of frequencies provided in the RTS would put many financial institutions with low-risk profiles or small size or non-complex nature in a difficult situation on their compliance journey with the regulation and its RTS. The purpose of Article 29 of the RTS remains unclear and requires further clarification. For the implementation of the EBA Guidelines on Outsourcing Arrangements, the regulator in Luxembourg (CSSF) adopted a clear approach in relation to the application of proportionality by bringing additional clarifications to the Guidelines when transposing the text into a circular: "In-Scope Entities shall, when complying with this Circular, have regard to the principle of proportionality. According to this principle, In-Scope Entities shall take implementing measures that are proportionate to their size and their internal organisation as well as to the nature, scale and complexity of their activities or services, including their risks. As such, In-Scope Entities that are large, complex or engage in risky activities or services shall adopt a more robust framework for their central administration, internal governance, and risk management. By contrast, In-Scope Entities may apply a less elaborated framework where justified by their size and internal organisation as well as by the nature, scale and complexity of their activities or services, including their risks.". In relation to the application of the proportionality principle, the regulator requires the documentation of the proportionality analysis in writing and have the conclusions approved by the management body under paragraph 6 of the Circular CSSF 22/806. It is suggested that a similar approach be followed in the RTS.
Q2: Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.

Not answered since the question is related to Simplified ICT RMF which has been kept out of scope.

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

No

Statements regarding the internal organisation of the three lines of defence (LoD) model might be confusing both in the RTS and the level 1 text. Specifically, Art. 6.4 of Regulation (EU) 2022/2554 says that responsibility for managing ICT risk should be assigned to a control function, but also that the ICT risk management function and control function should be segregated and independent. Literally, these statements are in conflict.

Further, some of the statements in Art 2 of the RTS (e.g., 1c) could be interpreted as forcing firms to locate their cybersecurity functions within the 2nd line of defence. Prescriptive requirements regarding which functions in a financial entity are located in which LoD should be avoided as many financial entities take different approaches in this regard. Further, prescriptive requirements in other jurisdictions could create a conflict of regulatory requirements that would be unmanageable for a financial entity. It is important to note that similar comments were made by the industry in response to the EBA's draft Guidelines on ICT and Security Risk Management 2019. The EBA made helpful clarifications in their final text and in the analysis of those comments (see page 73).

At last, RTS should avoid listing specific tasks which are to be carried out by specific functions. For example, Article 2.1.f says that the control function should develop ICT security awareness programmes and trainings. In many firms, these are developed by the cybersecurity function located within the 1LoD. This has benefits as it allows the financial entity to more easily incorporate relevant threat intelligence, for instance in the design of the financial entity phishing tests. While it is entirely possible that the control function could do this, and different financial entities will have different structures, it is more important that these trainings are designed well, and their effectiveness monitored, than that this is done by one function or another. Article 19 covers this sufficiently.

It is recommended that further clarity is provided by making additional statements in the recitals to the RTS which would provide legal clarity for financial entities who might otherwise feel compelled to interpret those statements literally. Suggested amendment to Recital 31 is as follows: "31. Article 2 of the proposed draft RTS details the minimum list of responsibilities to be assigned to the control function referred to in Article 6(4) of DORA. These RTS are not intended to prescribe to financial entities how to implement the lines of defence model for ICT and security risk management purposes, or to prescribe the location of certain functions within the 3 lines of defence model."

For Article 1, paragraph 1, in relation to the use of work "guarantee", it might not be possible to guarantee these requirements in all situations. Financial entities should put in place measures to reduce the risk that the events listed in this article do not occur, but in any ICT environment, it is possible that issues will arise and 100% availability cannot be guaranteed. It is suggested that the ESAs avoid reusing it if possible. The word "facilitate" is an alternative proposition.

Article 2, paragraph 1 f), it is suggested removing the word "developing" in order not to limit the freedom of institutions on awareness programme development. A control function should nevertheless monitor the effective implementation.

Q4. Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.
No Article 3, paragraph 3 requires financial institutions to update ICT risk management documentation where material changes to the cyber threat landscape occur. This may not be necessary in response to changes in the threat landscape, ICT services or ICT assets. The financial entity should rather consider whether such changes warrant any update to their policies and procedures, but these will not always be needed. It is suggested to add "as needed" to the sentence.
Q5. Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.
No The definition of "ICT asset" in the regulation is too broad (literally, a computer equipment such as mouse/keyboard might be considered an ICT asset). It is important for financial entities to take a proportionate approach to the mapping of ICT assets. In relation to Article 4, 2. (b) ii. and v. that cover all ICT assets and all legacy systems respectively, it suggested that the wording is adapted to ensure the proportionality principle is applied in Article 4, considering that some new technologies (e.g., serverless architecture) cannot easily be located to a specific jurisdiction and a legacy system which is going through decommissioning process might not require a risk assessment. In addition, it would be helpful to clarify that the RTS does not prescribe the creation of a single inventory or system of record. Such a clarification was given for the EBA ICT Risk Management Guidelines (page 94). While the ESAs expect financial entities to maintain inventories of more than just those ICT assets supporting critical or important functions, applying DORA's requirements to all ICT assets could have a negative impact on a financial entity's ability to manage risk. Hence, the proportionality principle is particularly relevant in allowing the financial entity to make decisions that make sense for its size and complexity and thereby facilitate good risk management. It is recommended that a wording line "In line with the proportionality principle in Article 4 of Regulation (EU) 2022/2554" is added in both Articles 4 and 5.
Q6. Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?
Yes While keeping record of the end date of the provider's support is important, this will not be possible or relevant for all ICT assets and it should be for the financial entity to determine the applicability of this requirement using a risk-based approach.
Q7. Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

No

Article 6, section 2.a lacks clarity in defining what constitutes 'data encryption in use.' It appears to mandate processing data in a separate and protected environment if encryption of data in use is not feasible. However, this requirement seems to be solely focused on processing data, without providing a clear rationale for the need for a separate protected environment. Additionally, this approach raises concerns as it may contradict other rules regarding the permissible data within a protected environment.

A suggestion for improvement would be to adopt a risk-based approach to determine whether data should be processed in a separate protected environment. This approach allows financial entities to evaluate the risks associated with processing data in various environments and make decisions based on the level of risk. Regulators should consider giving financial entities the opportunity to decide on the applicability of the requirement using the expression "where relevant". This allows organisations to define their own policy for specific situations based on their unique needs and circumstances. They can determine when and where the requirement is applicable, aligning it with their risk-based approach.

Recommended amendment to Article 6 (2) a "If encryption of data in use is not possible, financial entities shall consider, using a risk-based approach, whether to process data in use in a separated and protected environment to ensure the confidentiality, integrity and availability of data."

Article 7, (3) refers to the implementation of methods to recover lost keys. While technically this might not be possible to date, the paragraph should rather address the recovery of data in the case of lost, compromised or damaged keys.

Article 7, (4) refers to a register for all certificates and certificate storing devices. The text does not allow financial institutions to take a proportional and risk-based approach to this requirement. As currently written, this requirement is overly broad and likely not achievable for the vast majority of firms. For instance, all certificates would require the firm to have a register for certificates embedded in browsers, the scale of which is hard to calculate. It is suggested that the text is amended as "Financial entities shall create and maintain a register for all certificates and certificate storing devices deemed to be material to its digital operational resilience. The register shall be kept up-to date."

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

No

Given the level of requirements being already exhaustive, no new measure is deemed necessary.

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

No

Several policies and procedures may be found in operating procedures or running themes, and then, sometimes, they might overlap or share common goals. We suggest to echo the EBA risk balance of 2019, where authorities avoid prescribing where policies and procedures should be maintained within a financial entity. A similar approach on the management of policy/procedures.

The approach given in Art 8 covers areas that are typically the responsibility of teams wider than the security function. For instance, Art 8.1 states that ICT operating policies and procedures should be part of the ICT

security policies and procedures. However, ICT operating policies and procedures would typically be owned by the technology function, rather than the cybersecurity or ICT controls functions. It is suggested that the exact location within the organisation is not prescribed. We suggest to add a clarification to the recitals (e.g., in 53.) such as "This regulatory technical standard does not prescribe exactly where these policies and procedures should be maintained with the financial entity or which functions are responsible for individual requirements within this RTS.".

Equally important, it is suggested to add the proportionality principle in Recital 55.

For the Art 10 § 2.(b), we suggest to adopt a risk-based approach to determine the frequency of automated vulnerability scanning and assessments on ICT assets. The proposed approach would be to assess the criticality of the ICT asset itself and align the scanning frequency with its overall risk profile. It is suggested to remove the frequency of scans from the paragraph and add the risk-based approach.

Art 10, § 2.(c), the requirement states that financial entities must ensure that ICT third-party service providers (TPSP) handle any vulnerabilities related to the ICT services provided and report them. However, this reporting could lead to the financial entity being overwhelmed with vulnerability notifications. A more practical approach could be that ICT TPSP handle any vulnerabilities related to the ICT services and provide adequate assurance on the state of their vulnerability management and patching programs to the financial entity. The reporting could also focus on critical vulnerabilities with a risk-based approach. In addition, a clarification on the ICT TPSP is required in DORA regulation and relevant RTS documents. Services related to software licensing, all services provided within the financial institution's premises (e.g., ICT project management, development, help desk), ICT consulting activities, are suggested to be removed from the list of ICT services.

Art 10, § 2.(e), the disclosure of vulnerabilities to clients might lead to a loss of confidence. It is suggested that the wording limits the communication of vulnerabilities that could impact the clients and require an action from their side.

Art 10, § 4.(c), it is mentioned that financial entities should test and deploy software and hardware patches and updates in an environment that replicates the production one. This requirement may not be feasible especially in the case of critical security vulnerabilities. The risk-based approach should be considered. It is suggested to add in the text the wording of "where feasible" and "risk-based approach".". Proposal: "«test and deploy software and hardware patch and updates in an environment similar or representative, in terms of systems and patch levels, to the technologies deployed in production, to avoid adverse consequences and disruption before their deployment to production environment».

Art 11, § 2.(b), it should be noted that the requirement for baselines in EBA ICT and Security Risk Guidelines was limited to network components. Secure configuration may not be a relevant control for some ICT assets such as non-connected devices or very low risk assets. We suggest that financial entities apply a risk-based approach to this requirement and the text is amended to include risk-based approach.

Art 11, § 2.(i), there is a reference to data leakage prevention. This term is suggested to be replaced with the word "loss" to prevent confusion. It is important to note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (see commentary page 81) and replace it with data loss, which is a more appropriate term.

In Art 12, § 2, there is a prescriptive list of requirements. Instead, it would be beneficial to adjust the approach and adopt a more flexible stance. The EBA guidelines acknowledge that logging and monitoring are vital but emphasises that the implementation should be tailored to the institution's size and specific requirements on

p. 94. The statement would be "logging and monitoring are important and need to take place however the manner in which they are implemented shall be based on the institution proportionality approach". It is also suggested to amend Recital 60 accordingly".
Q10. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q11. What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.
No Concerning the automated vulnerability scans, we would recommend a monthly frequency for assets supporting critical and important functions and ad hoc scans could be conducted if necessary for critical vulnerability. Running weekly automated vulnerability scans on all ICT assets without considering the size, complexity and nature of the financial institutions as well as the resources needed to analyse the outcomes of the scans – all this will have a significant financial impact. The magnitude of costs will change whether the activity is outsourced or performed internally. In a context where a key provider like Microsoft publishes their patch updates monthly, a prescriptive frequency for running vulnerability scans not based on risk profile could be meaningless if the financial institution cannot address the identified vulnerabilities. The process should be based on documented risk analysis on different types of assets depending on their classification. The time, funds, and efforts for running automated scans on a weekly basis should be rather invested in improving the patch management process to address the vulnerabilities. The recommendation is against expanding the requirement to all ICT assets independent of their overall risk profile.
Q12. Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.
No While the requirements are clear, the challenge remains on finding suitable training for specific cloud solutions such as sector specific SaaS applications. What concerns Data and system security (Article 11): Understanding the global objectives of this article is compromised by the diversity of topics: requirements on access restrictions, secure configuration, malicious codes; data losses and leakage or cloud computing are listed in the same paragraph with no clear relation between them. We suggest the different security topics to be associated with the correspondent articles. For example, access restriction could be associated with Chapter II - Human resources policy and access control, Article 22. Article 11. (c) on software installation could be associated with Article 16 on systems acquisition, development, and maintenance.

Q13. Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.
No In Article 13, paragraph 1.(c), the approach could be complex to implement and disproportionate to the size of different type of financial institutions. It is suggested to bring proportionality principle in the text. In Article 13, paragraph 1.(h), the requirement for conducting firewall reviews twice a year for ICT systems supporting critical or important functions can be challenging for some entities due to the time it takes for them to complete the review, which might span up to 6 months. As a suggestion, it could be more practical to conduct firewall reviews at least once a year instead with ad-hoc scans following a major change. Furthermore, what this requirement lacks, is the consideration of the criticality of the system and a risk-based approach. Instead of mandating a fixed frequency for firewall reviews, the regulation should encourage financial entities to assess the criticality and risk profile of their systems and determine the appropriate review frequency accordingly. Systems with a higher risk profile may necessitate more frequent reviews, while lower-risk systems could be reviewed less often. In Article 14, paragraph 1, in relation to protecting information in transit, it is important to consider the financial entity's information classification system. For example, public information that is readily available does not need to be encrypted or subject to strenuous controls. In contrast, the transmission of PII or market sensitive data requires financial entities to consider strenuous controls to ensure the confidentiality and integrity of the data. It is suggested to amend the text "As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect the information in transit, considering the results of the approved data classification and the ICT risk assessment processes. In particular, financial entities shall ensure all of the following:" In Article 14, paragraph 1.(b), there is a reference to data leakage prevention. This term is suggested to be replaced with the word "loss" to prevent confusion. It is important to note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (see commentary page 81) and replace it with data loss, which is a more appropriate term.
Q14. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q15. Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.
No In relation to acquisition policy / procedure, while it is essential to address system acquisition, it is suggested to add that it may not necessarily fall under the one policy or procedure in the financial institutions. The requirements must be addressable in different policy / procedures.

Article 16, paragraph 1., it is quoted directly from the EBA guidelines (3.6.2 - Paragraph 1). However, the EBA guidelines include an additional sentence that states "this process should be designed using a risk-based approach." It is suggested that this sentence on adopting a risk-based approach is added to the text. Article 16, paragraph 2. (b), refer to independence for approving, requesting, and implementing the changes. This requirement might not be applicable to all types of changes. It is suggested that the text brings proportionality and risk-based approach to the requirement. The control cannot be applied consistently for a large institution with custom developed applications and for small institutions with commercial software. In addition, the size of the changes should be considered. Article 16, paragraph 4., does not introduce a risk-based approach for source code review. Applying the review type control for all developed software independent from the criticality or importance of the activity supported by the relevant application may not contribute to change management risks in a productive manner. Risk based approach is suggested to be introduced to the text. If testing the source code using static application security testing (SAST) is considered as good practice, more context is required about the operational possibility to deploy dynamic application security testing (DAST) for source code review. Article 16, paragraph 6., it would be complex to anonymize, pseudonymize or randomize the production data in all non-production environments. The requirement is suggested to be amended with risk-based approach considering that not all systems will contain confidential data. It is also suggested to make the link between Article 16.6 and 16.7 more explicit. Article 17, paragraph 2.(e) on fallback procedures is not risk based. It is suggested to be limited to major changes.
Q16. Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q17. Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.
No answer
Q18. Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.
Yes Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q19. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.

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

No

The scope for ICT personnel training requires flexibility, and the training programs should be adaptable based on functions and roles within the organisation. There are some uncertainties regarding certain training programs, such as digital operational resilience training, and their specific benefits to all staff. It is not clear to the industry what the practical difference is between ICT security and digital operational resilience training. It is essential to clarify the added value of these training courses compared to general security training. The regulation mandates also that the training should be applicable to all staff, but this broad scope may not be realistic or practical in some cases. A more targeted approach, focusing on specific roles and functions, can provide more effective and relevant training outcomes.

Furthermore, it is also unclear how a financial entity could include information on cryptographic techniques in its ICT security or digital operational resilience training. Such information is highly technical and would be irrelevant to all but highly specialist employees. The financial entity would also need to treat information regarding how it encrypts data with the appropriate caution, and details of those processes should not be widely shared within the entity. It is therefore suggested that this specific requirement be removed from the Article.

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

No

As currently drafted, the requirements in Article 20.1.b are to be extended to ICT third-party service providers. We do not believe this is practical or responsible from a risk management perspective. For instance, a third-party service provider cannot be expected to adhere to the financial entities' ICT security policies and procedures, nor would it make sense for them to do so as they would be tailored to the ICT environment of the financial entity. Therefore, it is suggested that "ICT third-party provider" is replaced by the term “contractor” in this context.

In the EBA guidelines, there was an amendment to replace the term "third party providers" with "contractors." This change might have been made to ensure that the requirement does not solely apply to legal entities but also includes any contracted parties providing services to the financial institution. By using the term "contractors," the scope of the requirement becomes broader and may include various service providers, not just legal entities. It is sensible to differentiate between contractors and internal staff, as certain security policies or sensitive information might not be shared with external contractors for security reasons.

In Article 21, paragraph 3.a, there seems to be confusion between the terms "third party provider" and "contractor." It is important to recognise that a unique identity requirement might not be feasible or reasonable for all third-party providers. The term "contractor" may have a different definition according to the EBA guidelines, and it is crucial to ensure that a unique identity requirement is appropriately adapted for different types of third-party relationships. In addition, it is suggested to provide a precise definition of “generic account”.

Regarding Article 22, 1.e.iv, it is suggested that the frequency is adopted to risk-based paragraph rather than being prescriptive, respecting at least annual review frequency. The same paragraph refers to the

performance of the review whenever a change is necessary at user level. This statement is not clear regarding the type of change at a user level. The type of change should be clarified. In addition, it is suggested that a clarification is brought in relation to the review of access role content (e.g., profile content) which is not covered in the RTS and DORA.
Q22. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q23. Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.
No The definition of an ICT-related incident could be interpreted broadly to include many incidents. For example, an employee losing access to home Wi-Fi while on a client call could be considered an adverse impact on the availability of the service provided by the financial entity. If all such incidents of negligible impact were to be in scope, then the documentation, classification and recording requirements in Article 23 would be overwhelming for a financial entity and would distract from good risk management. It is suggested that the text is amended for a financial entity to apply proportionality and a risk-based approach to its interpretation of what constitutes an ICT-related incident. In Article 23: -Paragraph 1.e, it is suggested that risk-based approach is introduced to the text considering the definition of ICT related incident is quite broad. -Paragraph 1.f, it might not be clear if it makes sense to review the ICT response and recovery plans against a range of different plausible scenarios. As the ICT response and recovery plans are already covered in Article 25 through 27, it is suggested that the sentence "The ICT response and recovery plans shall be reviewed against a range of different plausible scenarios." is removed from paragraph 1.f. In addition, rationale behind the requirements on annual review and update of the ICT-related incident management policy being not clear, it is suggested that the need to bring evolution and improvement to this policy is linked with the output of ICT risk management framework report required in Article 28. In Article 24, paragraph 2.a.ii, the term "usual scenarios of detection used by threat actors" and "scenarios based on threat intelligence activity" might be unclear. Further clarification is needed to define these terms and provide more specific guidance on the types of scenarios that financial entities should be prepared for. In that sense, it is important to highlight that EBA Guidelines on ICT and Security Risk 3.4.5 only required the identification of internal and external threats. It is suggested that the text "including usual scenarios of detection used by threat actors and scenarios " be removed from paragraph 2.a.ii. In Article 24, paragraph 2.b, while the implementation of tools might be costly related to the risks that small institutions are facing, it is recommended to bring the proportionality principle and risk-based approach in the text.

In Article 24, paragraph 2.c, as the text is currently drafted, it implies that the detection is management within an RTO, not the incident itself. Further, managing an incident within an RTO depends on a large number of factors in addition to detection time. Therefore, equating the two concepts is not appropriate here. We suggest removing the reference to managing an incident within RTO and adding the word "prompt" in front of detection to convey the expectation that alerts are considered and acted upon at an appropriate time.

In Article 24, paragraph 2.d, the text of this requirement is incomplete and therefore it is unclear what the expectation from financial entities is. The connection between scenarios and risks is not clear. It is suggested that the text be revised and completed by clearly describing the mapping between scenarios and logs.

In Article 24, paragraph 2.e, it is suggested that entities take a risk-based approach rather than analysing all information related to all anomalies. It is possible that the RTS overestimates the extent to which automated tooling can be relied on. Financial entities should prioritise based on risk, which is made up of several factors beyond only whether there is a connection to critical or important functions. In addition, the task might not be feasible for small size institution from a human resources and tools point of view.

In Article 24, paragraph 4, assuming there is a typo on the word "data", it is suggested to replace it with the word "date".

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

No

In the EBA guidelines, the term of ICT business continuity is referred in relation to disaster and recovery plans and to BIAs. We suggest that the definition is further clarified especially regarding to § 1(a) of the Art 25.

The approach and wording taken in DORA and the RTS are likely to create confusion between the ICT risk management framework, ICT resilience and recovery plans, and BCP. A BCP needs to be focused on the level of the business service, which may have any number of individual applications supporting it. The criteria for activating the technology recovery plans of an individual application are likely to be very different from activating the business continuity and recovery plans, as well as crisis management. These should be aligned and complimentary in how the financial entity builds resilience, for instance the RTO/RPO targets for an individual application need to support the RTO/RPO for the business they support. But recording them in the same document, or setting ownership within the same team, is often not scalable or helpful within a financial entity. Recital 92 attempts to clarify that the financial entity has some flexibility in how these are organised. However, we ask that the ESAs to clarify in Recital 92 that neither DORA nor the RTS mandate exactly where the information required in both the level 1 and level 2 texts is recorded within the financial entity so long as it is readily accessible and part of a coherent and holistic plan to deliver good resilience and risk management.

The articles' requirements depend on term "critical or important functions" in Art. 25, 1.(f)ii., or "critical functions" in Art. 26, 2.(a). We suggest to clarify whether there is a distinction between these two terms.

Art 26.2.a.: There is a need to take a risk-based approach to testing and the choice of scenarios given that the number of scenarios that could be tested will always greatly exceed the time and resources available to the financial entity (especially considering references to the scenarios given in Art 27.2). Which threat to test, the frequency that it is tested and the systems or infrastructure to be tested, must be a decision for the financial entity to take, balancing several risk factors. Impact and likelihood must remain the primary lens. Mandated scenarios could also result in firms navigating towards the same prescribed scenarios rather than taking a risk-based approach. We therefore recommend an amendment: Art 27.2: "The ICT response and recovery

plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The scenarios COULD include, BUT ARE NOT LIMITED TO, the following:" (to delete "shall" and "all of").

Scenarios that require the coordinated failure of many preventative controls for which there is no precedent cannot be considered plausible. Consideration of the threat profile, as well as ensuring plausibility, matters since, by focusing on scenarios which are implausible and which require the assumption of the failure of a great many controls, authorities risk driving attention toward areas where investment in resilience measures may be inefficient or ineffective in reducing risk compared to investment in preventative controls.

Regarding Art 26.2.b, the opportunity for ICT business continuity testing with third parties to gain qualitative and quantitative data for evidence to meet their recovery plans can be limited. It can be challenging for third parties to dedicate time and resources to bilateral testing with each of their customers. This issue is often a point of contention during contractual negotiations. We believe that it is important that financial entities can continue to rely on the assurances provided by third-party providers regarding their own ICT business continuity planning and testing regime, provided these are appropriate evidenced and meet the standards expected by the financial entity.

As to Art 27.1.b, the RTS uses the term critical ICT systems and services. This phrase is not defined in DORA and will create confusion regarding how to understand criticality. We recommend: Art 27.1.b, describes what actions shall be taken to "ensure the availability, integrity, continuity and recovery of at least the ICT systems SUPPORTING THE CRITICAL AND IMPORTANT FUNCTIONS of the financial entities;" (to delete "critical", "and services")

Art 27.4 creates a new category of ICT third-party provider of "key importance" to a financial "institutions" ICT service continuity. We believe this will create further definitional confusion by adding another layer or term of criticality and request that this requirement be aligned to terminology and requirements in the rest of the DORA text.

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

No

We are concerned about the potential negative implications of the 2-hour RTO requirement in Article 25.2.a. While this RTO is well established from the PFMIs, its applicability to the modern threat environment is questionable. We accept a 2-hour RTO as a target for non-malicious technology of business disruptions, but in the event of a disruption caused by malicious cybersecurity incident, we believe that a mandate to recover within 2 hours could drive CCPs and CSDs to attempt to recover outside of their risk appetite and before the necessary mitigation processes have been completed. We note that in their thematic findings to their 2022 Cyber Stress Test, the Bank of England noted that "*there might be instances where the disruption caused by an incident was such that, despite prior planning, attempting to recover by the end of the value date could have a more adverse impact on financial stability than failing to do so".* We support this finding and encourage EU authorities to consider the implications of a policy that may encourage financial entities to attempt to recover from a cybersecurity incident in such a way that the adverse impact to financial stability increases.

Regarding Article 25.4, zero data loss is not a realistic expectation. The ability to recover corrupted data depends among other things, on the frequency of the financial entity's backups. The financial entity may determine that it can tolerate an RPO of 12 hours for some data, but of 2 hours for others. It is also the case that the more frequent the financial entity backs up its data, the greater the likelihood that any corruption is copied to the back-up rendering the data unusable. A financial entity will need to balance these risks versus

investment in technologies such as data immutability. We recommend the following amendment: Article 25.4: "In addition to the requirements referred to in paragraph 1, trading venues shall ensure that its ICT business continuity arrangements allow trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any IT service of the trading venue after a disruptive incident is MINIMISED" (while deleting the phrase "close to zero").

Regarding Article 26.3-4, it may not always be appropriate to include members in the testing of ICT Business Continuity Plans. We recommend the inclusion of the phrase "where applicable", similar to the formula in Article 26.2.b.

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

No

As a general comment, the industry was surprised by the level of detail and the extent of the requirements expected for the report on the risk management framework. If the ESAs maintain this level of detail and frequency, we do not believe that conducting such a review and generating a report is workable objective for financial entities. This is for two reasons.

1. As noted elsewhere in our response, the RMF is in practice composed of a range of different policies, standards and activities. These are divided among a number of teams ranging across all three lines of defence. While a financial entity may adhere to all practices listed, these will not be collected and recorded in a single document or framework. Any review will therefore involve significant coordination across many colleagues which have different reporting lines and management committees. This will make the review a complex and labour-intensive process that will require a significant number of approvals from various internal governance forums and senior managers.
2. There are several different causes for conducting the review given in Article 6(5) of DORA. If each of these causes is triggered only once in a year, which is a conservative estimate, then the frequency of the reviews would easily outpace the speed with which a financial entity could complete them. This is particularly the case given the requirement for management body review and sign-off.

We recommend the ESAs reconsider the necessity of this level of reporting and evaluate its potential impact on competent authorities as well. We believe the reporting requirements will be redundant with certain already existing reporting to the regulator by the control functions such as the results of internal audits and is therefore questionable from an added value point of view.

Further, we anticipate that such reports would be very lengthy documents that would require significant time to review. We therefore question whether the competent authorities have allocated additional resource to this task or made allowances for the time required in the existing supervisory and exam schedule. It may lead to the opposite effect, overwhelming competent authorities with excessive data and potentially diminishing the efficiency of their oversight.

We therefore recommend that the ESAs consider shifting to a single review of the RMF that accounts for the activities of the preceding year in the areas in Art 6(5) of DORA. Anything more is likely to result in a material diversion of resources from existing governance and risk management, without adding any value to the financial entities own risk management practices.

Q27 – Q32

Not answered since the question is related to Simplified ICT RMF which has been kept out of scope.

Contacts: digital@abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA RTS to specify the policy on ICT services performed by ICT third-party providers

Date: 18 August 2023
EU Transparency register: 3505006282-58

General Drafting Principles
Q1. Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?
No Notwithstanding the availability of criteria in RTS, there is a need for more guidance on this matter. • The rank of subcontractors covered by the requirements should be specified. • The scope of third-party should be reduced in accordance with their risk level. • The requirements for exit plans should be more precise.
Q2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?
No There is a need for more guidance on how to enhance the existing policies with the new requirements. Instead of setting up a new individual policy again for this requirement focused on identifying the risks associated with the ICT dimension, we would welcome having the flexibility to set-up one common policy for Outsourcing and ICT and thus to have a global ICT framework in place. Furthermore, instead of having strict requirements we would prefer to have more guidance on how to focus on identifying risk dimension, to simplify the set up.
Q3. Question 3: Is article 4 appropriate and sufficiently clear?
No We suggest that the reference to a general location (without identifying the specific city) should be sufficient.
Q4. Is article 5 appropriate and sufficiently clear
Yes

Q5. Are articles 6 and 7 appropriate and sufficiently clear?
No We are of the opinion that the registration or authorisation by a competent authority should also be part of the due diligence assessment. We would welcome providing a definition of what is meant by "authorised entities". We would prefer to delete the obligation to assess "the ability of their providers to monitor relevant technological requirements" as they question the feasibility of doing such an assessment and that they do not see the rationale of this obligation. Ability to monitor: to have core objectives behind the criteria for due diligence; more freedom would be reasonable (e.g., cloud providers explaining their artificial intelligence (AI) systems). We are of the opinion that articles 7.2 and 7.3 are too prescriptive, more flexibility is needed.
Q6. Is article 8 appropriate and sufficiently clear?
Yes
Q7. Is article 9 appropriate and sufficiently clear?
Yes
Q8. Is article 10 appropriate and sufficiently clear?
No More clarification is needed on article 10 § 1 (drafting issue here). Relevant contractual arrangement is a defined term in the RTS. Meanwhile, it is unclear whether the special contractual agreements are meant here. Art 10 §2: What exactly are financial entities are expected to monitor here under the new regulation? We suggest amendments to article 10 § 2 in the way that financial entities monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant **principles.** We suggest using the Confidentiality, Integrity and Availability (CIA) ratings for individual providers.
Q9. Is article 11 appropriate and sufficiently clear?

No

Instead of requiring an exit plan for “each ICT service”, we suggest having one exit plan on each arrangement.

Feasibility of testing: We suggest requiring testing “when appropriate”.

Exit plans tests cannot be tested in real conditions. It would be more appropriate to perform regular desktop exercises to validate the exit plan.

Contacts: digital@abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA ITS to establish the templates for the register of information RTS on ICT risk management

Date: 18 August 2023
EU Transparency register: 3505006282-58

General Drafting Principles
Q1. Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?
Yes 1. Today, many ICT service providers do not have an LEI. This requirement goes beyond current industry requirements and practices and fails to consider the practical challenges of procuring LEIs, particularly across extensive supply chains which often comprise thousands of subcontractors. The proposed approach also overstates the general usefulness of LEIs to firms' TPO programs and risk management. 2. Even though the uniqueness of the identifier itself could be of sufficient use, there is no guarantee on the freshness and integrity of information associated to the identifier. In addition, it will require even more time if entities must verify themself information attached to the LEI. 3. The requirement to provision a LEI should be limited to material contractors of a given financial entity. 4. In this article it should be said explicitly that corporate data coming from an "active LEI" are deemed to be valid for inclusion into the register of Information 5. Quid of the ability of LEI organisation to deliver. Should they be consulted?
Q2: Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?
No This article requests a broader / deeper scrutiny on the chain of supplier without considering a risk-based approach and the principle of proportionality. The proposed definition of 'material subcontractors' risks an unnecessarily broad scope which does not properly reflect a risk-based approach. The materiality of subcontractor is subjective to a particular entity and a new concept introduced. We will suggest a re-wording to emphasise the listing of subcontractors supporting a material / critical function (business function) rather than all subcontractors. Scope should be limited to subcontractors providing a material part of the ICT service supporting a critical or important function, whose disruption or failure could materially impact the provision of the services.
Q3. When implementing the Register of Information for the first time: **▪ What would be the concrete necessary tasks and processes for the financial entities?** **▪ Are there any significant operational issues to consider?** **Please elaborate.**

Building a large cartography about contracts, ICT services, functions and providers and the obligation to update the information on a continuous basis involve a significant burden for regulated entities.

In fact, the points A to D refer to the second bullet point of the question.

a. Underlying approach to proportionality is unclear. The scope can be interpreted too broadly.
b. The maintenance and submission of registers is an very manual and tedious process that is prone to differences of definition or classification.
c. Managing contracts on the full chain is a significantly complex activity. It is not explicit in the text of ITS that the entity should stop the analysis at the first level of subcontractors.
d. The timing to implement the register of information is challenging.

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

No, but under the condition that historical agreements that have been terminated before the date of application of Regulation EU 2022/2554 should not be considered in the register of information. We suggest that the 5 years retention period should not be retroactive for terminated contracts.

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

No

The difficulty lies in the clarity to consolidate or sub-consolidate entities at EU level.

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

Main concern is about the workforce to maintain these registers. We see significant operational issues for these aspects.

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

No

We disagree because it is not clear what value this information brings to ESAs. The cost of an arrangement does not change its materiality or the concentration risk.

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

Yes

The template enables to capture the full complexity of the ICT value chain. However, we would like to underline that the effort to provide this information is not proportional to the gained information.

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

No

1. The taxonomy should be clarified and aligned with standard industry terminology (cf. NIST SP500-292). The rationale behind categories is unclear.
2. Some of the categories proposed in the taxonomy do not directly address the issues of resilience, e.g., presentation of advice, project, audit etc.
3. The word "provision" should be replaced by the world "rental" in all sentences. Provisioning does not fit with the ongoing nature of a service.
4. Definition is required to determine providers that could be qualified as data providers.
5. The scope of ICT services proposed in the taxonomy is very wide and should be reduced.

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

Yes

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

No

We observe challenges regarding sub-consolidation.

Furthermore, we suggest clarifying the different types of contracts (RT.01.01): standalone, overarching, and subsequent / associated arrangement.

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

We believe that the level of information is more than sufficient. However, the ITS is silent on whether additional fields could be added by national competent authorities (i.e., beyond the ultimate harmonised template).

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

No

There are some imprecisions, and several indicators are subjective (RT.99.01): data sensitiveness, discontinuing impact, services substitutability, and reintegration possibility.

Q14. Do you agree with the impact assessment and the main conclusions stemming from it? In addition to the consultation questions above, for each column of each template of the register of information, the following is asked:
a) Do you think the column should be kept? Y/N
b) Do you see a need to not amend the column? Y/N
c) Comments in case the answer to question (a) and/or question (b) "No".

Yes

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

General Notes to Take into account:

a. Overlap with GDPR, not so much at first glance.
b. Overlap with the existing register in Luxembourg (such as the one requested by CSSF), should the register maintain to keep track of all outsourcing not resulting from an arrangement with an ICT third-party service provider (BPO).

Contacts: digital@abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA RTS on ICT risk management framework and RTS on simplified ICT risk management framework

Date: 18 August 2023
EU Transparency register: 3505006282-58

General Drafting Principles
Q1. Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (Complexity and risks considerations)? If not, please provide detailed justifications and alternative wording as needed.
No While it is essential to incorporate proportionality in the RTS based on Article 15 of DORA, it is not possible to observe the proportionality principle being applied consistently on the entire RTS. Notably, when it comes to the frequency of certain controls, especially under Section V ICT Operations Security and Section VI Network Security, the prescriptive type of frequencies provided in the RTS would put many financial institutions with low-risk profiles or small size or non-complex nature in a difficult situation on their compliance journey with the regulation and its RTS. The purpose of Article 29 of the RTS remains unclear and requires further clarification. For the implementation of the EBA Guidelines on Outsourcing Arrangements, the regulator in Luxembourg (CSSF) adopted a clear approach in relation to the application of proportionality by bringing additional clarifications to the Guidelines when transposing the text into a circular: "In-Scope Entities shall, when complying with this Circular, have regard to the principle of proportionality. According to this principle, In-Scope Entities shall take implementing measures that are proportionate to their size and their internal organisation as well as to the nature, scale and complexity of their activities or services, including their risks. As such, In-Scope Entities that are large, complex or engage in risky activities or services shall adopt a more robust framework for their central administration, internal governance, and risk management. By contrast, In-Scope Entities may apply a less elaborated framework where justified by their size and internal organisation as well as by the nature, scale and complexity of their activities or services, including their risks.". In relation to the application of the proportionality principle, the regulator requires the documentation of the proportionality analysis in writing and have the conclusions approved by the management body under paragraph 6 of the Circular CSSF 22/806. It is suggested that a similar approach be followed in the RTS.
Q2: Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.

Not answered since the question is related to Simplified ICT RMF which has been kept out of scope.

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

No

Statements regarding the internal organisation of the three lines of defence (LoD) model might be confusing both in the RTS and the level 1 text. Specifically, Art. 6.4 of Regulation (EU) 2022/2554 says that responsibility for managing ICT risk should be assigned to a control function, but also that the ICT risk management function and control function should be segregated and independent. Literally, these statements are in conflict.

Further, some of the statements in Art 2 of the RTS (e.g., 1c) could be interpreted as forcing firms to locate their cybersecurity functions within the 2nd line of defence. Prescriptive requirements regarding which functions in a financial entity are located in which LoD should be avoided as many financial entities take different approaches in this regard. Further, prescriptive requirements in other jurisdictions could create a conflict of regulatory requirements that would be unmanageable for a financial entity. It is important to note that similar comments were made by the industry in response to the EBA's draft Guidelines on ICT and Security Risk Management 2019. The EBA made helpful clarifications in their final text and in the analysis of those comments (see page 73).

At last, RTS should avoid listing specific tasks which are to be carried out by specific functions. For example, Article 2.1.f says that the control function should develop ICT security awareness programmes and trainings. In many firms, these are developed by the cybersecurity function located within the 1LoD. This has benefits as it allows the financial entity to more easily incorporate relevant threat intelligence, for instance in the design of the financial entity phishing tests. While it is entirely possible that the control function could do this, and different financial entities will have different structures, it is more important that these trainings are designed well, and their effectiveness monitored, than that this is done by one function or another. Article 19 covers this sufficiently.

It is recommended that further clarity is provided by making additional statements in the recitals to the RTS which would provide legal clarity for financial entities who might otherwise feel compelled to interpret those statements literally. Suggested amendment to Recital 31 is as follows: "31. Article 2 of the proposed draft RTS details the minimum list of responsibilities to be assigned to the control function referred to in Article 6(4) of DORA. These RTS are not intended to prescribe to financial entities how to implement the lines of defence model for ICT and security risk management purposes, or to prescribe the location of certain functions within the 3 lines of defence model."

For Article 1, paragraph 1, in relation to the use of work "guarantee", it might not be possible to guarantee these requirements in all situations. Financial entities should put in place measures to reduce the risk that the events listed in this article do not occur, but in any ICT environment, it is possible that issues will arise and 100% availability cannot be guaranteed. It is suggested that the ESAs avoid reusing it if possible. The word "facilitate" is an alternative proposition.

Article 2, paragraph 1 f), it is suggested removing the word "developing" in order not to limit the freedom of institutions on awareness programme development. A control function should nevertheless monitor the effective implementation.

Q4. Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.
No Article 3, paragraph 3 requires financial institutions to update ICT risk management documentation where material changes to the cyber threat landscape occur. This may not be necessary in response to changes in the threat landscape, ICT services or ICT assets. The financial entity should rather consider whether such changes warrant any update to their policies and procedures, but these will not always be needed. It is suggested to add "as needed" to the sentence.
Q5. Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.
No The definition of "ICT asset" in the regulation is too broad (literally, a computer equipment such as mouse/keyboard might be considered an ICT asset). It is important for financial entities to take a proportionate approach to the mapping of ICT assets. In relation to Article 4, 2. (b) ii. and v. that cover all ICT assets and all legacy systems respectively, it suggested that the wording is adapted to ensure the proportionality principle is applied in Article 4, considering that some new technologies (e.g., serverless architecture) cannot easily be located to a specific jurisdiction and a legacy system which is going through decommissioning process might not require a risk assessment. In addition, it would be helpful to clarify that the RTS does not prescribe the creation of a single inventory or system of record. Such a clarification was given for the EBA ICT Risk Management Guidelines (page 94). While the ESAs expect financial entities to maintain inventories of more than just those ICT assets supporting critical or important functions, applying DORA's requirements to all ICT assets could have a negative impact on a financial entity's ability to manage risk. Hence, the proportionality principle is particularly relevant in allowing the financial entity to make decisions that make sense for its size and complexity and thereby facilitate good risk management. It is recommended that a wording line "In line with the proportionality principle in Article 4 of Regulation (EU) 2022/2554" is added in both Articles 4 and 5.
Q6. Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?
Yes While keeping record of the end date of the provider's support is important, this will not be possible or relevant for all ICT assets and it should be for the financial entity to determine the applicability of this requirement using a risk-based approach.
Q7. Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

No

Article 6, section 2.a lacks clarity in defining what constitutes 'data encryption in use.' It appears to mandate processing data in a separate and protected environment if encryption of data in use is not feasible. However, this requirement seems to be solely focused on processing data, without providing a clear rationale for the need for a separate protected environment. Additionally, this approach raises concerns as it may contradict other rules regarding the permissible data within a protected environment.

A suggestion for improvement would be to adopt a risk-based approach to determine whether data should be processed in a separate protected environment. This approach allows financial entities to evaluate the risks associated with processing data in various environments and make decisions based on the level of risk. Regulators should consider giving financial entities the opportunity to decide on the applicability of the requirement using the expression "where relevant". This allows organisations to define their own policy for specific situations based on their unique needs and circumstances. They can determine when and where the requirement is applicable, aligning it with their risk-based approach.

Recommended amendment to Article 6 (2) a "If encryption of data in use is not possible, financial entities shall consider, using a risk-based approach, whether to process data in use in a separated and protected environment to ensure the confidentiality, integrity and availability of data."

Article 7, (3) refers to the implementation of methods to recover lost keys. While technically this might not be possible to date, the paragraph should rather address the recovery of data in the case of lost, compromised or damaged keys.

Article 7, (4) refers to a register for all certificates and certificate storing devices. The text does not allow financial institutions to take a proportional and risk-based approach to this requirement. As currently written, this requirement is overly broad and likely not achievable for the vast majority of firms. For instance, all certificates would require the firm to have a register for certificates embedded in browsers, the scale of which is hard to calculate. It is suggested that the text is amended as "Financial entities shall create and maintain a register for all certificates and certificate storing devices deemed to be material to its digital operational resilience. The register shall be kept up-to date."

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

No

Given the level of requirements being already exhaustive, no new measure is deemed necessary.

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

No

Several policies and procedures may be found in operating procedures or running themes, and then, sometimes, they might overlap or share common goals. We suggest to echo the EBA risk balance of 2019, where authorities avoid prescribing where policies and procedures should be maintained within a financial entity. A similar approach on the management of policy/procedures.

The approach given in Art 8 covers areas that are typically the responsibility of teams wider than the security function. For instance, Art 8.1 states that ICT operating policies and procedures should be part of the ICT

security policies and procedures. However, ICT operating policies and procedures would typically be owned by the technology function, rather than the cybersecurity or ICT controls functions. It is suggested that the exact location within the organisation is not prescribed. We suggest to add a clarification to the recitals (e.g., in 53.) such as "This regulatory technical standard does not prescribe exactly where these policies and procedures should be maintained with the financial entity or which functions are responsible for individual requirements within this RTS.".

Equally important, it is suggested to add the proportionality principle in Recital 55.

For the Art 10 § 2.(b), we suggest to adopt a risk-based approach to determine the frequency of automated vulnerability scanning and assessments on ICT assets. The proposed approach would be to assess the criticality of the ICT asset itself and align the scanning frequency with its overall risk profile. It is suggested to remove the frequency of scans from the paragraph and add the risk-based approach.

Art 10, § 2.(c), the requirement states that financial entities must ensure that ICT third-party service providers (TPSP) handle any vulnerabilities related to the ICT services provided and report them. However, this reporting could lead to the financial entity being overwhelmed with vulnerability notifications. A more practical approach could be that ICT TPSP handle any vulnerabilities related to the ICT services and provide adequate assurance on the state of their vulnerability management and patching programs to the financial entity. The reporting could also focus on critical vulnerabilities with a risk-based approach. In addition, a clarification on the ICT TPSP is required in DORA regulation and relevant RTS documents. Services related to software licensing, all services provided within the financial institution's premises (e.g., ICT project management, development, help desk), ICT consulting activities, are suggested to be removed from the list of ICT services.

Art 10, § 2.(e), the disclosure of vulnerabilities to clients might lead to a loss of confidence. It is suggested that the wording limits the communication of vulnerabilities that could impact the clients and require an action from their side.

Art 10, § 4.(c), it is mentioned that financial entities should test and deploy software and hardware patches and updates in an environment that replicates the production one. This requirement may not be feasible especially in the case of critical security vulnerabilities. The risk-based approach should be considered. It is suggested to add in the text the wording of "where feasible" and "risk-based approach".". Proposal: "«test and deploy software and hardware patch and updates in an environment similar or representative, in terms of systems and patch levels, to the technologies deployed in production, to avoid adverse consequences and disruption before their deployment to production environment».

Art 11, § 2.(b), it should be noted that the requirement for baselines in EBA ICT and Security Risk Guidelines was limited to network components. Secure configuration may not be a relevant control for some ICT assets such as non-connected devices or very low risk assets. We suggest that financial entities apply a risk-based approach to this requirement and the text is amended to include risk-based approach.

Art 11, § 2.(i), there is a reference to data leakage prevention. This term is suggested to be replaced with the word "loss" to prevent confusion. It is important to note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (see commentary page 81) and replace it with data loss, which is a more appropriate term.

In Art 12, § 2, there is a prescriptive list of requirements. Instead, it would be beneficial to adjust the approach and adopt a more flexible stance. The EBA guidelines acknowledge that logging and monitoring are vital but emphasises that the implementation should be tailored to the institution's size and specific requirements on

p. 94. The statement would be "logging and monitoring are important and need to take place however the manner in which they are implemented shall be based on the institution proportionality approach". It is also suggested to amend Recital 60 accordingly".
Q10. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q11. What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.
No Concerning the automated vulnerability scans, we would recommend a monthly frequency for assets supporting critical and important functions and ad hoc scans could be conducted if necessary for critical vulnerability. Running weekly automated vulnerability scans on all ICT assets without considering the size, complexity and nature of the financial institutions as well as the resources needed to analyse the outcomes of the scans – all this will have a significant financial impact. The magnitude of costs will change whether the activity is outsourced or performed internally. In a context where a key provider like Microsoft publishes their patch updates monthly, a prescriptive frequency for running vulnerability scans not based on risk profile could be meaningless if the financial institution cannot address the identified vulnerabilities. The process should be based on documented risk analysis on different types of assets depending on their classification. The time, funds, and efforts for running automated scans on a weekly basis should be rather invested in improving the patch management process to address the vulnerabilities. The recommendation is against expanding the requirement to all ICT assets independent of their overall risk profile.
Q12. Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.
No While the requirements are clear, the challenge remains on finding suitable training for specific cloud solutions such as sector specific SaaS applications. What concerns Data and system security (Article 11): Understanding the global objectives of this article is compromised by the diversity of topics: requirements on access restrictions, secure configuration, malicious codes; data losses and leakage or cloud computing are listed in the same paragraph with no clear relation between them. We suggest the different security topics to be associated with the correspondent articles. For example, access restriction could be associated with Chapter II - Human resources policy and access control, Article 22. Article 11. (c) on software installation could be associated with Article 16 on systems acquisition, development, and maintenance.

Q13. Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.
No In Article 13, paragraph 1.(c), the approach could be complex to implement and disproportionate to the size of different type of financial institutions. It is suggested to bring proportionality principle in the text. In Article 13, paragraph 1.(h), the requirement for conducting firewall reviews twice a year for ICT systems supporting critical or important functions can be challenging for some entities due to the time it takes for them to complete the review, which might span up to 6 months. As a suggestion, it could be more practical to conduct firewall reviews at least once a year instead with ad-hoc scans following a major change. Furthermore, what this requirement lacks, is the consideration of the criticality of the system and a risk-based approach. Instead of mandating a fixed frequency for firewall reviews, the regulation should encourage financial entities to assess the criticality and risk profile of their systems and determine the appropriate review frequency accordingly. Systems with a higher risk profile may necessitate more frequent reviews, while lower-risk systems could be reviewed less often. In Article 14, paragraph 1, in relation to protecting information in transit, it is important to consider the financial entity's information classification system. For example, public information that is readily available does not need to be encrypted or subject to strenuous controls. In contrast, the transmission of PII or market sensitive data requires financial entities to consider strenuous controls to ensure the confidentiality and integrity of the data. It is suggested to amend the text "As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect the information in transit, considering the results of the approved data classification and the ICT risk assessment processes. In particular, financial entities shall ensure all of the following:" In Article 14, paragraph 1.(b), there is a reference to data leakage prevention. This term is suggested to be replaced with the word "loss" to prevent confusion. It is important to note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (see commentary page 81) and replace it with data loss, which is a more appropriate term.
Q14. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q15. Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.
No In relation to acquisition policy / procedure, while it is essential to address system acquisition, it is suggested to add that it may not necessarily fall under the one policy or procedure in the financial institutions. The requirements must be addressable in different policy / procedures.

Article 16, paragraph 1., it is quoted directly from the EBA guidelines (3.6.2 - Paragraph 1). However, the EBA guidelines include an additional sentence that states "this process should be designed using a risk-based approach." It is suggested that this sentence on adopting a risk-based approach is added to the text. Article 16, paragraph 2. (b), refer to independence for approving, requesting, and implementing the changes. This requirement might not be applicable to all types of changes. It is suggested that the text brings proportionality and risk-based approach to the requirement. The control cannot be applied consistently for a large institution with custom developed applications and for small institutions with commercial software. In addition, the size of the changes should be considered. Article 16, paragraph 4., does not introduce a risk-based approach for source code review. Applying the review type control for all developed software independent from the criticality or importance of the activity supported by the relevant application may not contribute to change management risks in a productive manner. Risk based approach is suggested to be introduced to the text. If testing the source code using static application security testing (SAST) is considered as good practice, more context is required about the operational possibility to deploy dynamic application security testing (DAST) for source code review. Article 16, paragraph 6., it would be complex to anonymize, pseudonymize or randomize the production data in all non-production environments. The requirement is suggested to be amended with risk-based approach considering that not all systems will contain confidential data. It is also suggested to make the link between Article 16.6 and 16.7 more explicit. Article 17, paragraph 2.(e) on fallback procedures is not risk based. It is suggested to be limited to major changes.
Q16. Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q17. Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.
No answer
Q18. Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.
Yes Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q19. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.

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

No

The scope for ICT personnel training requires flexibility, and the training programs should be adaptable based on functions and roles within the organisation. There are some uncertainties regarding certain training programs, such as digital operational resilience training, and their specific benefits to all staff. It is not clear to the industry what the practical difference is between ICT security and digital operational resilience training. It is essential to clarify the added value of these training courses compared to general security training. The regulation mandates also that the training should be applicable to all staff, but this broad scope may not be realistic or practical in some cases. A more targeted approach, focusing on specific roles and functions, can provide more effective and relevant training outcomes.

Furthermore, it is also unclear how a financial entity could include information on cryptographic techniques in its ICT security or digital operational resilience training. Such information is highly technical and would be irrelevant to all but highly specialist employees. The financial entity would also need to treat information regarding how it encrypts data with the appropriate caution, and details of those processes should not be widely shared within the entity. It is therefore suggested that this specific requirement be removed from the Article.

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

No

As currently drafted, the requirements in Article 20.1.b are to be extended to ICT third-party service providers. We do not believe this is practical or responsible from a risk management perspective. For instance, a third-party service provider cannot be expected to adhere to the financial entities' ICT security policies and procedures, nor would it make sense for them to do so as they would be tailored to the ICT environment of the financial entity. Therefore, it is suggested that "ICT third-party provider" is replaced by the term “contractor” in this context.

In the EBA guidelines, there was an amendment to replace the term "third party providers" with "contractors." This change might have been made to ensure that the requirement does not solely apply to legal entities but also includes any contracted parties providing services to the financial institution. By using the term "contractors," the scope of the requirement becomes broader and may include various service providers, not just legal entities. It is sensible to differentiate between contractors and internal staff, as certain security policies or sensitive information might not be shared with external contractors for security reasons.

In Article 21, paragraph 3.a, there seems to be confusion between the terms "third party provider" and "contractor." It is important to recognise that a unique identity requirement might not be feasible or reasonable for all third-party providers. The term "contractor" may have a different definition according to the EBA guidelines, and it is crucial to ensure that a unique identity requirement is appropriately adapted for different types of third-party relationships. In addition, it is suggested to provide a precise definition of “generic account”.

Regarding Article 22, 1.e.iv, it is suggested that the frequency is adopted to risk-based paragraph rather than being prescriptive, respecting at least annual review frequency. The same paragraph refers to the

performance of the review whenever a change is necessary at user level. This statement is not clear regarding the type of change at a user level. The type of change should be clarified. In addition, it is suggested that a clarification is brought in relation to the review of access role content (e.g., profile content) which is not covered in the RTS and DORA.
Q22. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q23. Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.
No The definition of an ICT-related incident could be interpreted broadly to include many incidents. For example, an employee losing access to home Wi-Fi while on a client call could be considered an adverse impact on the availability of the service provided by the financial entity. If all such incidents of negligible impact were to be in scope, then the documentation, classification and recording requirements in Article 23 would be overwhelming for a financial entity and would distract from good risk management. It is suggested that the text is amended for a financial entity to apply proportionality and a risk-based approach to its interpretation of what constitutes an ICT-related incident. In Article 23: -Paragraph 1.e, it is suggested that risk-based approach is introduced to the text considering the definition of ICT related incident is quite broad. -Paragraph 1.f, it might not be clear if it makes sense to review the ICT response and recovery plans against a range of different plausible scenarios. As the ICT response and recovery plans are already covered in Article 25 through 27, it is suggested that the sentence "The ICT response and recovery plans shall be reviewed against a range of different plausible scenarios." is removed from paragraph 1.f. In addition, rationale behind the requirements on annual review and update of the ICT-related incident management policy being not clear, it is suggested that the need to bring evolution and improvement to this policy is linked with the output of ICT risk management framework report required in Article 28. In Article 24, paragraph 2.a.ii, the term "usual scenarios of detection used by threat actors" and "scenarios based on threat intelligence activity" might be unclear. Further clarification is needed to define these terms and provide more specific guidance on the types of scenarios that financial entities should be prepared for. In that sense, it is important to highlight that EBA Guidelines on ICT and Security Risk 3.4.5 only required the identification of internal and external threats. It is suggested that the text "including usual scenarios of detection used by threat actors and scenarios " be removed from paragraph 2.a.ii. In Article 24, paragraph 2.b, while the implementation of tools might be costly related to the risks that small institutions are facing, it is recommended to bring the proportionality principle and risk-based approach in the text.

In Article 24, paragraph 2.c, as the text is currently drafted, it implies that the detection is management within an RTO, not the incident itself. Further, managing an incident within an RTO depends on a large number of factors in addition to detection time. Therefore, equating the two concepts is not appropriate here. We suggest removing the reference to managing an incident within RTO and adding the word "prompt" in front of detection to convey the expectation that alerts are considered and acted upon at an appropriate time.

In Article 24, paragraph 2.d, the text of this requirement is incomplete and therefore it is unclear what the expectation from financial entities is. The connection between scenarios and risks is not clear. It is suggested that the text be revised and completed by clearly describing the mapping between scenarios and logs.

In Article 24, paragraph 2.e, it is suggested that entities take a risk-based approach rather than analysing all information related to all anomalies. It is possible that the RTS overestimates the extent to which automated tooling can be relied on. Financial entities should prioritise based on risk, which is made up of several factors beyond only whether there is a connection to critical or important functions. In addition, the task might not be feasible for small size institution from a human resources and tools point of view.

In Article 24, paragraph 4, assuming there is a typo on the word "data", it is suggested to replace it with the word "date".

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

No

In the EBA guidelines, the term of ICT business continuity is referred in relation to disaster and recovery plans and to BIAs. We suggest that the definition is further clarified especially regarding to § 1(a) of the Art 25.

The approach and wording taken in DORA and the RTS are likely to create confusion between the ICT risk management framework, ICT resilience and recovery plans, and BCP. A BCP needs to be focused on the level of the business service, which may have any number of individual applications supporting it. The criteria for activating the technology recovery plans of an individual application are likely to be very different from activating the business continuity and recovery plans, as well as crisis management. These should be aligned and complimentary in how the financial entity builds resilience, for instance the RTO/RPO targets for an individual application need to support the RTO/RPO for the business they support. But recording them in the same document, or setting ownership within the same team, is often not scalable or helpful within a financial entity. Recital 92 attempts to clarify that the financial entity has some flexibility in how these are organised. However, we ask that the ESAs to clarify in Recital 92 that neither DORA nor the RTS mandate exactly where the information required in both the level 1 and level 2 texts is recorded within the financial entity so long as it is readily accessible and part of a coherent and holistic plan to deliver good resilience and risk management.

The articles' requirements depend on term "critical or important functions" in Art. 25, 1.(f)ii., or "critical functions" in Art. 26, 2.(a). We suggest to clarify whether there is a distinction between these two terms.

Art 26.2.a.: There is a need to take a risk-based approach to testing and the choice of scenarios given that the number of scenarios that could be tested will always greatly exceed the time and resources available to the financial entity (especially considering references to the scenarios given in Art 27.2). Which threat to test, the frequency that it is tested and the systems or infrastructure to be tested, must be a decision for the financial entity to take, balancing several risk factors. Impact and likelihood must remain the primary lens. Mandated scenarios could also result in firms navigating towards the same prescribed scenarios rather than taking a risk-based approach. We therefore recommend an amendment: Art 27.2: "The ICT response and recovery

plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The scenarios COULD include, BUT ARE NOT LIMITED TO, the following:" (to delete "shall" and "all of").

Scenarios that require the coordinated failure of many preventative controls for which there is no precedent cannot be considered plausible. Consideration of the threat profile, as well as ensuring plausibility, matters since, by focusing on scenarios which are implausible and which require the assumption of the failure of a great many controls, authorities risk driving attention toward areas where investment in resilience measures may be inefficient or ineffective in reducing risk compared to investment in preventative controls.

Regarding Art 26.2.b, the opportunity for ICT business continuity testing with third parties to gain qualitative and quantitative data for evidence to meet their recovery plans can be limited. It can be challenging for third parties to dedicate time and resources to bilateral testing with each of their customers. This issue is often a point of contention during contractual negotiations. We believe that it is important that financial entities can continue to rely on the assurances provided by third-party providers regarding their own ICT business continuity planning and testing regime, provided these are appropriate evidenced and meet the standards expected by the financial entity.

As to Art 27.1.b, the RTS uses the term critical ICT systems and services. This phrase is not defined in DORA and will create confusion regarding how to understand criticality. We recommend: Art 27.1.b, describes what actions shall be taken to "ensure the availability, integrity, continuity and recovery of at least the ICT systems SUPPORTING THE CRITICAL AND IMPORTANT FUNCTIONS of the financial entities;" (to delete "critical", "and services")

Art 27.4 creates a new category of ICT third-party provider of "key importance" to a financial "institutions" ICT service continuity. We believe this will create further definitional confusion by adding another layer or term of criticality and request that this requirement be aligned to terminology and requirements in the rest of the DORA text.

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

No

We are concerned about the potential negative implications of the 2-hour RTO requirement in Article 25.2.a. While this RTO is well established from the PFMIs, its applicability to the modern threat environment is questionable. We accept a 2-hour RTO as a target for non-malicious technology of business disruptions, but in the event of a disruption caused by malicious cybersecurity incident, we believe that a mandate to recover within 2 hours could drive CCPs and CSDs to attempt to recover outside of their risk appetite and before the necessary mitigation processes have been completed. We note that in their thematic findings to their 2022 Cyber Stress Test, the Bank of England noted that "*there might be instances where the disruption caused by an incident was such that, despite prior planning, attempting to recover by the end of the value date could have a more adverse impact on financial stability than failing to do so".* We support this finding and encourage EU authorities to consider the implications of a policy that may encourage financial entities to attempt to recover from a cybersecurity incident in such a way that the adverse impact to financial stability increases.

Regarding Article 25.4, zero data loss is not a realistic expectation. The ability to recover corrupted data depends among other things, on the frequency of the financial entity's backups. The financial entity may determine that it can tolerate an RPO of 12 hours for some data, but of 2 hours for others. It is also the case that the more frequent the financial entity backs up its data, the greater the likelihood that any corruption is copied to the back-up rendering the data unusable. A financial entity will need to balance these risks versus

investment in technologies such as data immutability. We recommend the following amendment: Article 25.4: "In addition to the requirements referred to in paragraph 1, trading venues shall ensure that its ICT business continuity arrangements allow trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any IT service of the trading venue after a disruptive incident is MINIMISED" (while deleting the phrase "close to zero").

Regarding Article 26.3-4, it may not always be appropriate to include members in the testing of ICT Business Continuity Plans. We recommend the inclusion of the phrase "where applicable", similar to the formula in Article 26.2.b.

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

No

As a general comment, the industry was surprised by the level of detail and the extent of the requirements expected for the report on the risk management framework. If the ESAs maintain this level of detail and frequency, we do not believe that conducting such a review and generating a report is workable objective for financial entities. This is for two reasons.

1. As noted elsewhere in our response, the RMF is in practice composed of a range of different policies, standards and activities. These are divided among a number of teams ranging across all three lines of defence. While a financial entity may adhere to all practices listed, these will not be collected and recorded in a single document or framework. Any review will therefore involve significant coordination across many colleagues which have different reporting lines and management committees. This will make the review a complex and labour-intensive process that will require a significant number of approvals from various internal governance forums and senior managers.
2. There are several different causes for conducting the review given in Article 6(5) of DORA. If each of these causes is triggered only once in a year, which is a conservative estimate, then the frequency of the reviews would easily outpace the speed with which a financial entity could complete them. This is particularly the case given the requirement for management body review and sign-off.

We recommend the ESAs reconsider the necessity of this level of reporting and evaluate its potential impact on competent authorities as well. We believe the reporting requirements will be redundant with certain already existing reporting to the regulator by the control functions such as the results of internal audits and is therefore questionable from an added value point of view.

Further, we anticipate that such reports would be very lengthy documents that would require significant time to review. We therefore question whether the competent authorities have allocated additional resource to this task or made allowances for the time required in the existing supervisory and exam schedule. It may lead to the opposite effect, overwhelming competent authorities with excessive data and potentially diminishing the efficiency of their oversight.

We therefore recommend that the ESAs consider shifting to a single review of the RMF that accounts for the activities of the preceding year in the areas in Art 6(5) of DORA. Anything more is likely to result in a material diversion of resources from existing governance and risk management, without adding any value to the financial entities own risk management practices.

Q27 – Q32

Not answered since the question is related to Simplified ICT RMF which has been kept out of scope.

Contacts: digital@abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA RTS on criteria for the classification of ICT-related incidents

Date: 18 August 2023

EU Transparency register: 3505006282-58

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.

No

Reasoning:

While the approach for classifying major incidents seems relevant, it is challenging to classify ICT incident as major as all types of daily incident must undergo the assessment under these criteria and across different jurisdiction of the entity. The definition of ICT-related incident could be interpreted broadly to include a large number of incidents. For example, an employee losing to access to home Wi-Fi while on a client call could be considered an adverse impact on the availability of the service provided by the financial entity. If all such incidents of negligeable impact were to be in scope, then the documentation, classification and recording requirements in Article 23 would be overwhelming for a financial entity and would distract from good risk management. We therefore believe that it is necessary for a financial entity to apply proportionality and a risk-based approach to its interpretation of what constitutes an ICT-related incident.

In addition, not only the thresholds seem to be in certain cases too low or too broad but the information to be collected is hard to obtain, in particular, when it comes to other jurisdictions, clients or other financial counterparts.

We do agree on the approach on the condition that the criteria are revised.

Regarding the approach for classification: it is an overly complex approach based on estimations that could lead to over-declaration and non-harmonisation of practices. The assessment takes time away from the resolution of the incident itself.

What concerns the first report: the timeframe to fill it in should be at least 72 hours, to allow the entity to conduct the required assessment.

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.

No

Too many materialisations, unknown information (e.g., volume of customers impacted / volume of customers using all the assets/services of an IT estate). Using estimates will lead to biases and create room for interpretations.

Reasoning:

Art 1. 3. Firms do not have access to the information that would allow for the assessment of impact on clients or financial counterparts or the subsequent impact that would have on objectives and market efficiency.
Art. 1. 5. 'Comparable reference period' is imprecise. Language should make it clear that the firm is responsible for determining a 'reference period' to base estimates off and will not be held responsible for inaccurate estimates.
Art 9. 1. A. This is set at the PSD2 lower impact threshold but is considered a primary indicator in DORA (10% vs 25%). A lower limit may give rise to additional reporting particularly where it is triggered by 2 or more primary criteria having been met. We would suggest maintaining 25% threshold.
Art 9. 1. C/E. These seem to be arbitrary numbers pulled from PSD2 (a regulation primarily directed to retail banks) yet they are not reflective of what would be considered a major incident for a wholesale bank where a single impacted transaction within the Bank is very likely to breach the EUR 15 million limit. This is a weakness in the current MIR process that we would be keen to see addressed. The percentage criterion is more logical as it can be applied consistently regardless of the size of the institution (i.e., 25% of transactions affected is likely to be a material issue whether you are a small regional bank or a global wholesale bank whereas EUR 15million impact will significantly differ). However, if an absolute number is needed, we would recommend as high as negotiable, maybe 100,000 clients and EUR 30,000,000.
Art 9. 1. F 'Any impact' can be interpreted to include non-critical operations and would lead to over-reporting, especially if firms are expected to estimate because of the lack of access to appropriate information on the appropriate timeline. As stated above, firms do not have access that would allow for the assessment of impact on clients or financial counterparts or the subsequent impact that would have on objectives and market efficiency.

Suggestions:

Article 1.f: We suggest removing this sentence:

~~"3. In relation to the relevance of clients and/or financial counterparts, the financial entity shall take into account the extent to which the impact on a client and/or a financial counterpart will affect the implementation of the business objectives of the financial entity, as well as the potential impact of the incident on market efficiency."~~

Article 5f
5. "Where the actual number of clients, financial counterparts or number or amount of transactions impacted cannot be determined, the financial entity shall use estimates based on available data" while removing the last phrase "from comparable reference periods."

Article 9.1:
a) the number of affected clients is higher than 25% of all clients using the affected service of the financial entity; or
c) the number of affected clients is higher than 100,000 clients; or
f) We suggest removing this phrase: "~~any identified impact on relevant clients or financial counterpart in accordance with Article 1(3)"~~

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.

No

Reasoning:

Art 2. 1. 'Attract media attention,' 'received complaints,' and 'lose clients' are too broad and will lead to over-reporting. We suggest limiting the assessment of 'reputation impact' to the time of the incident to avoid over-reporting caused by criteria being subsequently met in hindsight after the incident. We also suggest applying here the DORA Article 4 Proportionality Principal.
Art 2. C. The financial entity is likely not to meet regulatory requirements' needs to be further qualified. Technically, most incidents could result in missed regulatory requirements. PSD2 MIR qualifies this categorisation as "regulatory requirements have not been complied with, resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available." We suggest similar language is included here.
Art 11. B. There can be an outage of services that support critical or important functions without that downtime impacting those specifically critical or important functions. This could lead to over-reporting incidents that do not impact critical and important functions. We suggest making the impact to critical or important functions explicit.
Art 4 A/C Firms do not have access to the external information at the time of an incident that would allow them to assess the impact on their clients and/or counterparts operations in different territories. It is quite impossible to gather information on impact in other EU member states. Over-reporting will occur if financial entities are expected to guess if a common third party is impacted in different territories.
Art 12 'Materiality' is not reflected in this language, and we recommend amending the article to include it.
Art 15.1. This limit is too low and will lead to over-reporting. While Article 7.2 does state that BAU costs should not be included in this calculation does, it is unclear if any technology costs related to fixing an incident to return it to its original state fall under this BAU category. An absolute cost closer to EUR 250,000 would be more appropriate. In addition, this initiative could lead to the transfer of ICT services outside of the EU where costs are lower and therefore threshold never met.

Suggestions:

Article 2
Classification criterion 'Reputational impact'
(1) For the purposes of determining the reputational impact of the incident, considering the PROPORTIONALITY PRINCIPAL, financial entities shall take into account the level of visibility that the incident has gained in the market. In particular, financial entities shall, within reason, consider whether one of the following are MET AT THE TIME OF THE INCIDENT:

Article 11
b) the duration of the incident IS LONGER THAN TWO HOURS FOR A CRITICAL OR IMPORTANT FUNCTION, without prejudice to stricter availability and recovery

Article 4

We suggest removing the following paragraphs "a" and "c":

~~"a) The clients and financial counterparts affected; or"~~

~~"c) Financial market infrastructures or third-party providers that may be common with other financial entities"~~

Article 12
Any MATERIAL impact of the incident in the territories of at least two Member States in accordance with Article 4 shall be considered as meeting the threshold of the criterion for major ICT-incidents under Article 8(3)(c).

Article 15

Economic impact: We suggest replacing the absolute threshold by allowing each entity to define the relevant applicable threshold based on its size and overall risk profile, and the nature, scale and complexity of its services, activities, and operations. The entity could explain the rationale behind the determination of the threshold in a dedicated policy. Alternatively, the materiality threshold of the economic impact in accordance with Article 7 is met where the gross direct and indirect costs and losses incurred by the financial entity from the major incident have exceeded or are likely to exceed EUR 250,000~~.~~

Reputational impact: The scope of media relevant for this criterion should be more precise (for example the scope proposed by the ECB: "national or international media coverage in major newspapers or news agencies such as the Financial Times, Reuters, Bloomberg or national equivalents of large audience"

Service downtime: The threshold should be set in accordance with business needs by the financial entity. Proposal: "the service downtime is longer, for ICT services supporting critical functions, than the threshold set by the entity in accordance with its BIA, its SLA and its size and overall risk profile, and the nature, scale and complexity of its services, activities and operations, without prejudice to stricter availability and recovery requirements set out in Regulation (EU) 2022/2554 and other EU legislation."

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.

No

Reasoning:

The definition and the threshold of the criterion 'Data losses' should be explained.

Art 13 'Any significant impact' is too broad and will lead to over-reporting. The financial entity itself should be responsible for determining what level of 'data loss' is significant and therefore determining a quantitative threshold.

Suggestions:

Article 13
Materiality thresholds for the classification criterion 'Data losses'

Any significant impact AS DETERMINED BY THE FINANCIAL ENTITY in accordance with Article 5 on availability, authenticity, integrity, or confidentiality of critical data, which would have an adverse impact on the implementation of the business objectives of the financial entity or on meeting regulatory requirements shall be considered as meeting the thresholds of the criterion for major incidents under Article 8(2)(b).

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.

No

Reasoning:

This is an important criterion, but it must be correlated with the length of downtime in order to take the impact into account. A 10 minute delay in opening a critical service does not necessarily lead to a major incident. There is a very high risk of over-reporting. Addition of the criterion «brought to the attention of the management body» is not very relevant, criteria need to be aligned with DORA requirements.

Art 14 This language exceeds the level 1 mandate of 'the criticality of the services affected, including the financial entity's transactions and operations.'
Besides, we suggest to:
- specify and make it explicit what exactly authorisation/registration in the EU means
- add the word "formally" to the escalation process to Senior Management or Management Body

Suggestions:

Article 14

Materiality thresholds for the classification criterion 'Critical services affected'.

Any impact on critical services in accordance with Article 6, which has been formally escalated by the financial entity to its senior management or management body shall be considered as meeting the threshold of the criterion for major incidents under Article 8(2)(c).

The notification of the management body threshold should be replaced by: "Any impact on critical services in accordance with Article 6, which has been escalated by the financial entity to AMSB and is mobilizing a crisis unit within the entity, shall be considered as meeting the threshold of the criterion for major incidents under article 8(2)(c)."

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).

No

Reasoning:

Art 16. 2.

This entails excessive analysis and correlation workload, and hence leading to a high-risk of over-reporting, with minor incidents occurring twice. Extending the period to 6-12 months would further amplify the phenomenon. It would be more relevant to apply to incidents that are not major but still have relatively significant impact.

Two unrelated incidents may appear related at first and such criterion will lead to over-reporting unrelated incidents. We suggest increasing the number of incidents that determine recurring.

Determining whether this criterion has been met when triaging an issue to make a reportability decision is likely to be extremely challenging and burdensome since the root cause is unlikely to be known at the time. Similarly, nature and impact are not precise and will lead to over-reporting. We suggest narrowing criteria to impacting critical or important functions.

Suggestions:

This notion does not appear in level 1 and seem irrelevant, therefore should be deleted.

Article 16

2. For the purposes of paragraph 1, recurring incidents shall occur at least FOUR TIMES, have the same apparent root cause and shall be with similar nature and impact TO CRITICAL OR IMPORTANT FUNCTIONS.

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.

No

Reasoning:

We do not believe it is possible for a financial entity to assess impacts or effects on other financial entities, third-party providers, clients or counterparts.

In **Art 17.1.a**, almost any cyber threat could in theory affect the CIF of any financial entity, third-party provider, clients or financial counterparts, as this depends on the details of their control environment and unique risk profile. No financial entity could assess those factors, and therefore this criterion would trigger for any and all cyber threats known to the financial entity.

We believe it is better to limit cyber threat analysis to the financial entity itself and not expect any analysis of other entities. While many firms will monitor threats and may become aware of threats to another financial entity, this is done on an ad-hoc basis, mostly based on threat intelligence. Mandating this would like to detract for the focus on threats targeted at the financial entity itself and ultimately be a distraction for all but the best resourced entities.

In Art. 17.1.b, it is not possible for a financial entity to assess probability of materialisation at other financial entities. In particular, the elements given in Art 17.2, a financial entity is not privy to the information required in points A and C and so could not take them into account.

We believe it is better to limit cyber threat analysis to the financial entity itself and not expect any analysis of other entities. While many firms will monitor threats and may become aware of threats to another financial entity, this is done on an ad-hoc basis, mostly based on threat intelligence. Mandating this would detract from the focus on threats targeted at the financial entity itself and ultimately be a distraction for all but the best resourced entities.

We also suggest the introduction and reference to NIS2.

Suggestions:

Article 17
1. For the purposes Article 18(2) of Regulation (EU) 2022/2554, a cyber threat shall be significant, where it fulfils ALL the following conditions:

a) the cyber threat could affect critical or important functions of the financial entity. Here, we suggest removing this phrase: ", ~~other financial entities, third-party providers, clients or financial counterparts.~~"

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.

No

Reasoning:

The risks of spill-over and contagion are born by security incidents, not by IT production incidents. Production incidents should be excluded from this article.

We agree to share lessons learned and major incidents characteristics, but not infrastructure details, systems used or impacted, and etc.

Contacts: digital@abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA RTS to specify the policy on ICT services performed by ICT third-party providers

Date: 18 August 2023
EU Transparency register: 3505006282-58

General Drafting Principles
Q1. Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?
No Notwithstanding the availability of criteria in RTS, there is a need for more guidance on this matter. • The rank of subcontractors covered by the requirements should be specified. • The scope of third-party should be reduced in accordance with their risk level. • The requirements for exit plans should be more precise.
Q2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?
No There is a need for more guidance on how to enhance the existing policies with the new requirements. Instead of setting up a new individual policy again for this requirement focused on identifying the risks associated with the ICT dimension, we would welcome having the flexibility to set-up one common policy for Outsourcing and ICT and thus to have a global ICT framework in place. Furthermore, instead of having strict requirements we would prefer to have more guidance on how to focus on identifying risk dimension, to simplify the set up.
Q3. Question 3: Is article 4 appropriate and sufficiently clear?
No We suggest that the reference to a general location (without identifying the specific city) should be sufficient.
Q4. Is article 5 appropriate and sufficiently clear
Yes

Q5. Are articles 6 and 7 appropriate and sufficiently clear?
No We are of the opinion that the registration or authorisation by a competent authority should also be part of the due diligence assessment. We would welcome providing a definition of what is meant by "authorised entities". We would prefer to delete the obligation to assess "the ability of their providers to monitor relevant technological requirements" as they question the feasibility of doing such an assessment and that they do not see the rationale of this obligation. Ability to monitor: to have core objectives behind the criteria for due diligence; more freedom would be reasonable (e.g., cloud providers explaining their artificial intelligence (AI) systems). We are of the opinion that articles 7.2 and 7.3 are too prescriptive, more flexibility is needed.
Q6. Is article 8 appropriate and sufficiently clear?
Yes
Q7. Is article 9 appropriate and sufficiently clear?
Yes
Q8. Is article 10 appropriate and sufficiently clear?
No More clarification is needed on article 10 § 1 (drafting issue here). Relevant contractual arrangement is a defined term in the RTS. Meanwhile, it is unclear whether the special contractual agreements are meant here. Art 10 §2: What exactly are financial entities are expected to monitor here under the new regulation? We suggest amendments to article 10 § 2 in the way that financial entities monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant **principles.** We suggest using the Confidentiality, Integrity and Availability (CIA) ratings for individual providers.
Q9. Is article 11 appropriate and sufficiently clear?

No

Instead of requiring an exit plan for “each ICT service”, we suggest having one exit plan on each arrangement.

Feasibility of testing: We suggest requiring testing “when appropriate”.

Exit plans tests cannot be tested in real conditions. It would be more appropriate to perform regular desktop exercises to validate the exit plan.

Contacts: digital@abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA ITS to establish the templates for the register of information RTS on ICT risk management

Date: 18 August 2023
EU Transparency register: 3505006282-58

General Drafting Principles
Q1. Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?
Yes 1. Today, many ICT service providers do not have an LEI. This requirement goes beyond current industry requirements and practices and fails to consider the practical challenges of procuring LEIs, particularly across extensive supply chains which often comprise thousands of subcontractors. The proposed approach also overstates the general usefulness of LEIs to firms' TPO programs and risk management. 2. Even though the uniqueness of the identifier itself could be of sufficient use, there is no guarantee on the freshness and integrity of information associated to the identifier. In addition, it will require even more time if entities must verify themself information attached to the LEI. 3. The requirement to provision a LEI should be limited to material contractors of a given financial entity. 4. In this article it should be said explicitly that corporate data coming from an "active LEI" are deemed to be valid for inclusion into the register of Information 5. Quid of the ability of LEI organisation to deliver. Should they be consulted?
Q2: Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?
No This article requests a broader / deeper scrutiny on the chain of supplier without considering a risk-based approach and the principle of proportionality. The proposed definition of 'material subcontractors' risks an unnecessarily broad scope which does not properly reflect a risk-based approach. The materiality of subcontractor is subjective to a particular entity and a new concept introduced. We will suggest a re-wording to emphasise the listing of subcontractors supporting a material / critical function (business function) rather than all subcontractors. Scope should be limited to subcontractors providing a material part of the ICT service supporting a critical or important function, whose disruption or failure could materially impact the provision of the services.
Q3. When implementing the Register of Information for the first time: **▪ What would be the concrete necessary tasks and processes for the financial entities?** **▪ Are there any significant operational issues to consider?** **Please elaborate.**

Building a large cartography about contracts, ICT services, functions and providers and the obligation to update the information on a continuous basis involve a significant burden for regulated entities.

In fact, the points A to D refer to the second bullet point of the question.

a. Underlying approach to proportionality is unclear. The scope can be interpreted too broadly.
b. The maintenance and submission of registers is an very manual and tedious process that is prone to differences of definition or classification.
c. Managing contracts on the full chain is a significantly complex activity. It is not explicit in the text of ITS that the entity should stop the analysis at the first level of subcontractors.
d. The timing to implement the register of information is challenging.

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

No, but under the condition that historical agreements that have been terminated before the date of application of Regulation EU 2022/2554 should not be considered in the register of information. We suggest that the 5 years retention period should not be retroactive for terminated contracts.

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

No

The difficulty lies in the clarity to consolidate or sub-consolidate entities at EU level.

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

Main concern is about the workforce to maintain these registers. We see significant operational issues for these aspects.

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

No

We disagree because it is not clear what value this information brings to ESAs. The cost of an arrangement does not change its materiality or the concentration risk.

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

Yes

The template enables to capture the full complexity of the ICT value chain. However, we would like to underline that the effort to provide this information is not proportional to the gained information.

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

No

1. The taxonomy should be clarified and aligned with standard industry terminology (cf. NIST SP500-292). The rationale behind categories is unclear.
2. Some of the categories proposed in the taxonomy do not directly address the issues of resilience, e.g., presentation of advice, project, audit etc.
3. The word "provision" should be replaced by the world "rental" in all sentences. Provisioning does not fit with the ongoing nature of a service.
4. Definition is required to determine providers that could be qualified as data providers.
5. The scope of ICT services proposed in the taxonomy is very wide and should be reduced.

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

Yes

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

No

We observe challenges regarding sub-consolidation.

Furthermore, we suggest clarifying the different types of contracts (RT.01.01): standalone, overarching, and subsequent / associated arrangement.

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

We believe that the level of information is more than sufficient. However, the ITS is silent on whether additional fields could be added by national competent authorities (i.e., beyond the ultimate harmonised template).

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

No

There are some imprecisions, and several indicators are subjective (RT.99.01): data sensitiveness, discontinuing impact, services substitutability, and reintegration possibility.

Q14. Do you agree with the impact assessment and the main conclusions stemming from it? In addition to the consultation questions above, for each column of each template of the register of information, the following is asked:
a) Do you think the column should be kept? Y/N
b) Do you see a need to not amend the column? Y/N
c) Comments in case the answer to question (a) and/or question (b) "No".

Yes

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

General Notes to Take into account:

a. Overlap with GDPR, not so much at first glance.
b. Overlap with the existing register in Luxembourg (such as the one requested by CSSF), should the register maintain to keep track of all outsourcing not resulting from an arrangement with an ICT third-party service provider (BPO).

Contacts: digital@abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA RTS on ICT risk management framework and RTS on simplified ICT risk management framework

Date: 18 August 2023
EU Transparency register: 3505006282-58

General Drafting Principles
Q1. Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (Complexity and risks considerations)? If not, please provide detailed justifications and alternative wording as needed.
No While it is essential to incorporate proportionality in the RTS based on Article 15 of DORA, it is not possible to observe the proportionality principle being applied consistently on the entire RTS. Notably, when it comes to the frequency of certain controls, especially under Section V ICT Operations Security and Section VI Network Security, the prescriptive type of frequencies provided in the RTS would put many financial institutions with low-risk profiles or small size or non-complex nature in a difficult situation on their compliance journey with the regulation and its RTS. The purpose of Article 29 of the RTS remains unclear and requires further clarification. For the implementation of the EBA Guidelines on Outsourcing Arrangements, the regulator in Luxembourg (CSSF) adopted a clear approach in relation to the application of proportionality by bringing additional clarifications to the Guidelines when transposing the text into a circular: "In-Scope Entities shall, when complying with this Circular, have regard to the principle of proportionality. According to this principle, In-Scope Entities shall take implementing measures that are proportionate to their size and their internal organisation as well as to the nature, scale and complexity of their activities or services, including their risks. As such, In-Scope Entities that are large, complex or engage in risky activities or services shall adopt a more robust framework for their central administration, internal governance, and risk management. By contrast, In-Scope Entities may apply a less elaborated framework where justified by their size and internal organisation as well as by the nature, scale and complexity of their activities or services, including their risks.". In relation to the application of the proportionality principle, the regulator requires the documentation of the proportionality analysis in writing and have the conclusions approved by the management body under paragraph 6 of the Circular CSSF 22/806. It is suggested that a similar approach be followed in the RTS.
Q2: Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.

Not answered since the question is related to Simplified ICT RMF which has been kept out of scope.

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

No

Statements regarding the internal organisation of the three lines of defence (LoD) model might be confusing both in the RTS and the level 1 text. Specifically, Art. 6.4 of Regulation (EU) 2022/2554 says that responsibility for managing ICT risk should be assigned to a control function, but also that the ICT risk management function and control function should be segregated and independent. Literally, these statements are in conflict.

Further, some of the statements in Art 2 of the RTS (e.g., 1c) could be interpreted as forcing firms to locate their cybersecurity functions within the 2nd line of defence. Prescriptive requirements regarding which functions in a financial entity are located in which LoD should be avoided as many financial entities take different approaches in this regard. Further, prescriptive requirements in other jurisdictions could create a conflict of regulatory requirements that would be unmanageable for a financial entity. It is important to note that similar comments were made by the industry in response to the EBA's draft Guidelines on ICT and Security Risk Management 2019. The EBA made helpful clarifications in their final text and in the analysis of those comments (see page 73).

At last, RTS should avoid listing specific tasks which are to be carried out by specific functions. For example, Article 2.1.f says that the control function should develop ICT security awareness programmes and trainings. In many firms, these are developed by the cybersecurity function located within the 1LoD. This has benefits as it allows the financial entity to more easily incorporate relevant threat intelligence, for instance in the design of the financial entity phishing tests. While it is entirely possible that the control function could do this, and different financial entities will have different structures, it is more important that these trainings are designed well, and their effectiveness monitored, than that this is done by one function or another. Article 19 covers this sufficiently.

It is recommended that further clarity is provided by making additional statements in the recitals to the RTS which would provide legal clarity for financial entities who might otherwise feel compelled to interpret those statements literally. Suggested amendment to Recital 31 is as follows: "31. Article 2 of the proposed draft RTS details the minimum list of responsibilities to be assigned to the control function referred to in Article 6(4) of DORA. These RTS are not intended to prescribe to financial entities how to implement the lines of defence model for ICT and security risk management purposes, or to prescribe the location of certain functions within the 3 lines of defence model."

For Article 1, paragraph 1, in relation to the use of work "guarantee", it might not be possible to guarantee these requirements in all situations. Financial entities should put in place measures to reduce the risk that the events listed in this article do not occur, but in any ICT environment, it is possible that issues will arise and 100% availability cannot be guaranteed. It is suggested that the ESAs avoid reusing it if possible. The word "facilitate" is an alternative proposition.

Article 2, paragraph 1 f), it is suggested removing the word "developing" in order not to limit the freedom of institutions on awareness programme development. A control function should nevertheless monitor the effective implementation.

Q4. Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.
No Article 3, paragraph 3 requires financial institutions to update ICT risk management documentation where material changes to the cyber threat landscape occur. This may not be necessary in response to changes in the threat landscape, ICT services or ICT assets. The financial entity should rather consider whether such changes warrant any update to their policies and procedures, but these will not always be needed. It is suggested to add "as needed" to the sentence.
Q5. Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.
No The definition of "ICT asset" in the regulation is too broad (literally, a computer equipment such as mouse/keyboard might be considered an ICT asset). It is important for financial entities to take a proportionate approach to the mapping of ICT assets. In relation to Article 4, 2. (b) ii. and v. that cover all ICT assets and all legacy systems respectively, it suggested that the wording is adapted to ensure the proportionality principle is applied in Article 4, considering that some new technologies (e.g., serverless architecture) cannot easily be located to a specific jurisdiction and a legacy system which is going through decommissioning process might not require a risk assessment. In addition, it would be helpful to clarify that the RTS does not prescribe the creation of a single inventory or system of record. Such a clarification was given for the EBA ICT Risk Management Guidelines (page 94). While the ESAs expect financial entities to maintain inventories of more than just those ICT assets supporting critical or important functions, applying DORA's requirements to all ICT assets could have a negative impact on a financial entity's ability to manage risk. Hence, the proportionality principle is particularly relevant in allowing the financial entity to make decisions that make sense for its size and complexity and thereby facilitate good risk management. It is recommended that a wording line "In line with the proportionality principle in Article 4 of Regulation (EU) 2022/2554" is added in both Articles 4 and 5.
Q6. Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?
Yes While keeping record of the end date of the provider's support is important, this will not be possible or relevant for all ICT assets and it should be for the financial entity to determine the applicability of this requirement using a risk-based approach.
Q7. Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

No

Article 6, section 2.a lacks clarity in defining what constitutes 'data encryption in use.' It appears to mandate processing data in a separate and protected environment if encryption of data in use is not feasible. However, this requirement seems to be solely focused on processing data, without providing a clear rationale for the need for a separate protected environment. Additionally, this approach raises concerns as it may contradict other rules regarding the permissible data within a protected environment.

A suggestion for improvement would be to adopt a risk-based approach to determine whether data should be processed in a separate protected environment. This approach allows financial entities to evaluate the risks associated with processing data in various environments and make decisions based on the level of risk. Regulators should consider giving financial entities the opportunity to decide on the applicability of the requirement using the expression "where relevant". This allows organisations to define their own policy for specific situations based on their unique needs and circumstances. They can determine when and where the requirement is applicable, aligning it with their risk-based approach.

Recommended amendment to Article 6 (2) a "If encryption of data in use is not possible, financial entities shall consider, using a risk-based approach, whether to process data in use in a separated and protected environment to ensure the confidentiality, integrity and availability of data."

Article 7, (3) refers to the implementation of methods to recover lost keys. While technically this might not be possible to date, the paragraph should rather address the recovery of data in the case of lost, compromised or damaged keys.

Article 7, (4) refers to a register for all certificates and certificate storing devices. The text does not allow financial institutions to take a proportional and risk-based approach to this requirement. As currently written, this requirement is overly broad and likely not achievable for the vast majority of firms. For instance, all certificates would require the firm to have a register for certificates embedded in browsers, the scale of which is hard to calculate. It is suggested that the text is amended as "Financial entities shall create and maintain a register for all certificates and certificate storing devices deemed to be material to its digital operational resilience. The register shall be kept up-to date."

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

No

Given the level of requirements being already exhaustive, no new measure is deemed necessary.

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

No

Several policies and procedures may be found in operating procedures or running themes, and then, sometimes, they might overlap or share common goals. We suggest to echo the EBA risk balance of 2019, where authorities avoid prescribing where policies and procedures should be maintained within a financial entity. A similar approach on the management of policy/procedures.

The approach given in Art 8 covers areas that are typically the responsibility of teams wider than the security function. For instance, Art 8.1 states that ICT operating policies and procedures should be part of the ICT

security policies and procedures. However, ICT operating policies and procedures would typically be owned by the technology function, rather than the cybersecurity or ICT controls functions. It is suggested that the exact location within the organisation is not prescribed. We suggest to add a clarification to the recitals (e.g., in 53.) such as "This regulatory technical standard does not prescribe exactly where these policies and procedures should be maintained with the financial entity or which functions are responsible for individual requirements within this RTS.".

Equally important, it is suggested to add the proportionality principle in Recital 55.

For the Art 10 § 2.(b), we suggest to adopt a risk-based approach to determine the frequency of automated vulnerability scanning and assessments on ICT assets. The proposed approach would be to assess the criticality of the ICT asset itself and align the scanning frequency with its overall risk profile. It is suggested to remove the frequency of scans from the paragraph and add the risk-based approach.

Art 10, § 2.(c), the requirement states that financial entities must ensure that ICT third-party service providers (TPSP) handle any vulnerabilities related to the ICT services provided and report them. However, this reporting could lead to the financial entity being overwhelmed with vulnerability notifications. A more practical approach could be that ICT TPSP handle any vulnerabilities related to the ICT services and provide adequate assurance on the state of their vulnerability management and patching programs to the financial entity. The reporting could also focus on critical vulnerabilities with a risk-based approach. In addition, a clarification on the ICT TPSP is required in DORA regulation and relevant RTS documents. Services related to software licensing, all services provided within the financial institution's premises (e.g., ICT project management, development, help desk), ICT consulting activities, are suggested to be removed from the list of ICT services.

Art 10, § 2.(e), the disclosure of vulnerabilities to clients might lead to a loss of confidence. It is suggested that the wording limits the communication of vulnerabilities that could impact the clients and require an action from their side.

Art 10, § 4.(c), it is mentioned that financial entities should test and deploy software and hardware patches and updates in an environment that replicates the production one. This requirement may not be feasible especially in the case of critical security vulnerabilities. The risk-based approach should be considered. It is suggested to add in the text the wording of "where feasible" and "risk-based approach".". Proposal: "«test and deploy software and hardware patch and updates in an environment similar or representative, in terms of systems and patch levels, to the technologies deployed in production, to avoid adverse consequences and disruption before their deployment to production environment».

Art 11, § 2.(b), it should be noted that the requirement for baselines in EBA ICT and Security Risk Guidelines was limited to network components. Secure configuration may not be a relevant control for some ICT assets such as non-connected devices or very low risk assets. We suggest that financial entities apply a risk-based approach to this requirement and the text is amended to include risk-based approach.

Art 11, § 2.(i), there is a reference to data leakage prevention. This term is suggested to be replaced with the word "loss" to prevent confusion. It is important to note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (see commentary page 81) and replace it with data loss, which is a more appropriate term.

In Art 12, § 2, there is a prescriptive list of requirements. Instead, it would be beneficial to adjust the approach and adopt a more flexible stance. The EBA guidelines acknowledge that logging and monitoring are vital but emphasises that the implementation should be tailored to the institution's size and specific requirements on

p. 94. The statement would be "logging and monitoring are important and need to take place however the manner in which they are implemented shall be based on the institution proportionality approach". It is also suggested to amend Recital 60 accordingly".
Q10. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q11. What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.
No Concerning the automated vulnerability scans, we would recommend a monthly frequency for assets supporting critical and important functions and ad hoc scans could be conducted if necessary for critical vulnerability. Running weekly automated vulnerability scans on all ICT assets without considering the size, complexity and nature of the financial institutions as well as the resources needed to analyse the outcomes of the scans – all this will have a significant financial impact. The magnitude of costs will change whether the activity is outsourced or performed internally. In a context where a key provider like Microsoft publishes their patch updates monthly, a prescriptive frequency for running vulnerability scans not based on risk profile could be meaningless if the financial institution cannot address the identified vulnerabilities. The process should be based on documented risk analysis on different types of assets depending on their classification. The time, funds, and efforts for running automated scans on a weekly basis should be rather invested in improving the patch management process to address the vulnerabilities. The recommendation is against expanding the requirement to all ICT assets independent of their overall risk profile.
Q12. Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.
No While the requirements are clear, the challenge remains on finding suitable training for specific cloud solutions such as sector specific SaaS applications. What concerns Data and system security (Article 11): Understanding the global objectives of this article is compromised by the diversity of topics: requirements on access restrictions, secure configuration, malicious codes; data losses and leakage or cloud computing are listed in the same paragraph with no clear relation between them. We suggest the different security topics to be associated with the correspondent articles. For example, access restriction could be associated with Chapter II - Human resources policy and access control, Article 22. Article 11. (c) on software installation could be associated with Article 16 on systems acquisition, development, and maintenance.

Q13. Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.
No In Article 13, paragraph 1.(c), the approach could be complex to implement and disproportionate to the size of different type of financial institutions. It is suggested to bring proportionality principle in the text. In Article 13, paragraph 1.(h), the requirement for conducting firewall reviews twice a year for ICT systems supporting critical or important functions can be challenging for some entities due to the time it takes for them to complete the review, which might span up to 6 months. As a suggestion, it could be more practical to conduct firewall reviews at least once a year instead with ad-hoc scans following a major change. Furthermore, what this requirement lacks, is the consideration of the criticality of the system and a risk-based approach. Instead of mandating a fixed frequency for firewall reviews, the regulation should encourage financial entities to assess the criticality and risk profile of their systems and determine the appropriate review frequency accordingly. Systems with a higher risk profile may necessitate more frequent reviews, while lower-risk systems could be reviewed less often. In Article 14, paragraph 1, in relation to protecting information in transit, it is important to consider the financial entity's information classification system. For example, public information that is readily available does not need to be encrypted or subject to strenuous controls. In contrast, the transmission of PII or market sensitive data requires financial entities to consider strenuous controls to ensure the confidentiality and integrity of the data. It is suggested to amend the text "As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect the information in transit, considering the results of the approved data classification and the ICT risk assessment processes. In particular, financial entities shall ensure all of the following:" In Article 14, paragraph 1.(b), there is a reference to data leakage prevention. This term is suggested to be replaced with the word "loss" to prevent confusion. It is important to note that the EBA chose to remove the term from its 2019 Guidelines on ICT and Security Risk management (see commentary page 81) and replace it with data loss, which is a more appropriate term.
Q14. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q15. Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.
No In relation to acquisition policy / procedure, while it is essential to address system acquisition, it is suggested to add that it may not necessarily fall under the one policy or procedure in the financial institutions. The requirements must be addressable in different policy / procedures.

Article 16, paragraph 1., it is quoted directly from the EBA guidelines (3.6.2 - Paragraph 1). However, the EBA guidelines include an additional sentence that states "this process should be designed using a risk-based approach." It is suggested that this sentence on adopting a risk-based approach is added to the text. Article 16, paragraph 2. (b), refer to independence for approving, requesting, and implementing the changes. This requirement might not be applicable to all types of changes. It is suggested that the text brings proportionality and risk-based approach to the requirement. The control cannot be applied consistently for a large institution with custom developed applications and for small institutions with commercial software. In addition, the size of the changes should be considered. Article 16, paragraph 4., does not introduce a risk-based approach for source code review. Applying the review type control for all developed software independent from the criticality or importance of the activity supported by the relevant application may not contribute to change management risks in a productive manner. Risk based approach is suggested to be introduced to the text. If testing the source code using static application security testing (SAST) is considered as good practice, more context is required about the operational possibility to deploy dynamic application security testing (DAST) for source code review. Article 16, paragraph 6., it would be complex to anonymize, pseudonymize or randomize the production data in all non-production environments. The requirement is suggested to be amended with risk-based approach considering that not all systems will contain confidential data. It is also suggested to make the link between Article 16.6 and 16.7 more explicit. Article 17, paragraph 2.(e) on fallback procedures is not risk based. It is suggested to be limited to major changes.
Q16. Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q17. Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.
No answer
Q18. Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.
Yes Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q19. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.

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

No

The scope for ICT personnel training requires flexibility, and the training programs should be adaptable based on functions and roles within the organisation. There are some uncertainties regarding certain training programs, such as digital operational resilience training, and their specific benefits to all staff. It is not clear to the industry what the practical difference is between ICT security and digital operational resilience training. It is essential to clarify the added value of these training courses compared to general security training. The regulation mandates also that the training should be applicable to all staff, but this broad scope may not be realistic or practical in some cases. A more targeted approach, focusing on specific roles and functions, can provide more effective and relevant training outcomes.

Furthermore, it is also unclear how a financial entity could include information on cryptographic techniques in its ICT security or digital operational resilience training. Such information is highly technical and would be irrelevant to all but highly specialist employees. The financial entity would also need to treat information regarding how it encrypts data with the appropriate caution, and details of those processes should not be widely shared within the entity. It is therefore suggested that this specific requirement be removed from the Article.

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

No

As currently drafted, the requirements in Article 20.1.b are to be extended to ICT third-party service providers. We do not believe this is practical or responsible from a risk management perspective. For instance, a third-party service provider cannot be expected to adhere to the financial entities' ICT security policies and procedures, nor would it make sense for them to do so as they would be tailored to the ICT environment of the financial entity. Therefore, it is suggested that "ICT third-party provider" is replaced by the term “contractor” in this context.

In the EBA guidelines, there was an amendment to replace the term "third party providers" with "contractors." This change might have been made to ensure that the requirement does not solely apply to legal entities but also includes any contracted parties providing services to the financial institution. By using the term "contractors," the scope of the requirement becomes broader and may include various service providers, not just legal entities. It is sensible to differentiate between contractors and internal staff, as certain security policies or sensitive information might not be shared with external contractors for security reasons.

In Article 21, paragraph 3.a, there seems to be confusion between the terms "third party provider" and "contractor." It is important to recognise that a unique identity requirement might not be feasible or reasonable for all third-party providers. The term "contractor" may have a different definition according to the EBA guidelines, and it is crucial to ensure that a unique identity requirement is appropriately adapted for different types of third-party relationships. In addition, it is suggested to provide a precise definition of “generic account”.

Regarding Article 22, 1.e.iv, it is suggested that the frequency is adopted to risk-based paragraph rather than being prescriptive, respecting at least annual review frequency. The same paragraph refers to the

performance of the review whenever a change is necessary at user level. This statement is not clear regarding the type of change at a user level. The type of change should be clarified. In addition, it is suggested that a clarification is brought in relation to the review of access role content (e.g., profile content) which is not covered in the RTS and DORA.
Q22. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
No Given the level of requirements being already exhaustive, no new measure is deemed necessary.
Q23. Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.
No The definition of an ICT-related incident could be interpreted broadly to include many incidents. For example, an employee losing access to home Wi-Fi while on a client call could be considered an adverse impact on the availability of the service provided by the financial entity. If all such incidents of negligible impact were to be in scope, then the documentation, classification and recording requirements in Article 23 would be overwhelming for a financial entity and would distract from good risk management. It is suggested that the text is amended for a financial entity to apply proportionality and a risk-based approach to its interpretation of what constitutes an ICT-related incident. In Article 23: -Paragraph 1.e, it is suggested that risk-based approach is introduced to the text considering the definition of ICT related incident is quite broad. -Paragraph 1.f, it might not be clear if it makes sense to review the ICT response and recovery plans against a range of different plausible scenarios. As the ICT response and recovery plans are already covered in Article 25 through 27, it is suggested that the sentence "The ICT response and recovery plans shall be reviewed against a range of different plausible scenarios." is removed from paragraph 1.f. In addition, rationale behind the requirements on annual review and update of the ICT-related incident management policy being not clear, it is suggested that the need to bring evolution and improvement to this policy is linked with the output of ICT risk management framework report required in Article 28. In Article 24, paragraph 2.a.ii, the term "usual scenarios of detection used by threat actors" and "scenarios based on threat intelligence activity" might be unclear. Further clarification is needed to define these terms and provide more specific guidance on the types of scenarios that financial entities should be prepared for. In that sense, it is important to highlight that EBA Guidelines on ICT and Security Risk 3.4.5 only required the identification of internal and external threats. It is suggested that the text "including usual scenarios of detection used by threat actors and scenarios " be removed from paragraph 2.a.ii. In Article 24, paragraph 2.b, while the implementation of tools might be costly related to the risks that small institutions are facing, it is recommended to bring the proportionality principle and risk-based approach in the text.

In Article 24, paragraph 2.c, as the text is currently drafted, it implies that the detection is management within an RTO, not the incident itself. Further, managing an incident within an RTO depends on a large number of factors in addition to detection time. Therefore, equating the two concepts is not appropriate here. We suggest removing the reference to managing an incident within RTO and adding the word "prompt" in front of detection to convey the expectation that alerts are considered and acted upon at an appropriate time.

In Article 24, paragraph 2.d, the text of this requirement is incomplete and therefore it is unclear what the expectation from financial entities is. The connection between scenarios and risks is not clear. It is suggested that the text be revised and completed by clearly describing the mapping between scenarios and logs.

In Article 24, paragraph 2.e, it is suggested that entities take a risk-based approach rather than analysing all information related to all anomalies. It is possible that the RTS overestimates the extent to which automated tooling can be relied on. Financial entities should prioritise based on risk, which is made up of several factors beyond only whether there is a connection to critical or important functions. In addition, the task might not be feasible for small size institution from a human resources and tools point of view.

In Article 24, paragraph 4, assuming there is a typo on the word "data", it is suggested to replace it with the word "date".

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

No

In the EBA guidelines, the term of ICT business continuity is referred in relation to disaster and recovery plans and to BIAs. We suggest that the definition is further clarified especially regarding to § 1(a) of the Art 25.

The approach and wording taken in DORA and the RTS are likely to create confusion between the ICT risk management framework, ICT resilience and recovery plans, and BCP. A BCP needs to be focused on the level of the business service, which may have any number of individual applications supporting it. The criteria for activating the technology recovery plans of an individual application are likely to be very different from activating the business continuity and recovery plans, as well as crisis management. These should be aligned and complimentary in how the financial entity builds resilience, for instance the RTO/RPO targets for an individual application need to support the RTO/RPO for the business they support. But recording them in the same document, or setting ownership within the same team, is often not scalable or helpful within a financial entity. Recital 92 attempts to clarify that the financial entity has some flexibility in how these are organised. However, we ask that the ESAs to clarify in Recital 92 that neither DORA nor the RTS mandate exactly where the information required in both the level 1 and level 2 texts is recorded within the financial entity so long as it is readily accessible and part of a coherent and holistic plan to deliver good resilience and risk management.

The articles' requirements depend on term "critical or important functions" in Art. 25, 1.(f)ii., or "critical functions" in Art. 26, 2.(a). We suggest to clarify whether there is a distinction between these two terms.

Art 26.2.a.: There is a need to take a risk-based approach to testing and the choice of scenarios given that the number of scenarios that could be tested will always greatly exceed the time and resources available to the financial entity (especially considering references to the scenarios given in Art 27.2). Which threat to test, the frequency that it is tested and the systems or infrastructure to be tested, must be a decision for the financial entity to take, balancing several risk factors. Impact and likelihood must remain the primary lens. Mandated scenarios could also result in firms navigating towards the same prescribed scenarios rather than taking a risk-based approach. We therefore recommend an amendment: Art 27.2: "The ICT response and recovery

plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The scenarios COULD include, BUT ARE NOT LIMITED TO, the following:" (to delete "shall" and "all of").

Scenarios that require the coordinated failure of many preventative controls for which there is no precedent cannot be considered plausible. Consideration of the threat profile, as well as ensuring plausibility, matters since, by focusing on scenarios which are implausible and which require the assumption of the failure of a great many controls, authorities risk driving attention toward areas where investment in resilience measures may be inefficient or ineffective in reducing risk compared to investment in preventative controls.

Regarding Art 26.2.b, the opportunity for ICT business continuity testing with third parties to gain qualitative and quantitative data for evidence to meet their recovery plans can be limited. It can be challenging for third parties to dedicate time and resources to bilateral testing with each of their customers. This issue is often a point of contention during contractual negotiations. We believe that it is important that financial entities can continue to rely on the assurances provided by third-party providers regarding their own ICT business continuity planning and testing regime, provided these are appropriate evidenced and meet the standards expected by the financial entity.

As to Art 27.1.b, the RTS uses the term critical ICT systems and services. This phrase is not defined in DORA and will create confusion regarding how to understand criticality. We recommend: Art 27.1.b, describes what actions shall be taken to "ensure the availability, integrity, continuity and recovery of at least the ICT systems SUPPORTING THE CRITICAL AND IMPORTANT FUNCTIONS of the financial entities;" (to delete "critical", "and services")

Art 27.4 creates a new category of ICT third-party provider of "key importance" to a financial "institutions" ICT service continuity. We believe this will create further definitional confusion by adding another layer or term of criticality and request that this requirement be aligned to terminology and requirements in the rest of the DORA text.

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

No

We are concerned about the potential negative implications of the 2-hour RTO requirement in Article 25.2.a. While this RTO is well established from the PFMIs, its applicability to the modern threat environment is questionable. We accept a 2-hour RTO as a target for non-malicious technology of business disruptions, but in the event of a disruption caused by malicious cybersecurity incident, we believe that a mandate to recover within 2 hours could drive CCPs and CSDs to attempt to recover outside of their risk appetite and before the necessary mitigation processes have been completed. We note that in their thematic findings to their 2022 Cyber Stress Test, the Bank of England noted that "*there might be instances where the disruption caused by an incident was such that, despite prior planning, attempting to recover by the end of the value date could have a more adverse impact on financial stability than failing to do so".* We support this finding and encourage EU authorities to consider the implications of a policy that may encourage financial entities to attempt to recover from a cybersecurity incident in such a way that the adverse impact to financial stability increases.

Regarding Article 25.4, zero data loss is not a realistic expectation. The ability to recover corrupted data depends among other things, on the frequency of the financial entity's backups. The financial entity may determine that it can tolerate an RPO of 12 hours for some data, but of 2 hours for others. It is also the case that the more frequent the financial entity backs up its data, the greater the likelihood that any corruption is copied to the back-up rendering the data unusable. A financial entity will need to balance these risks versus

investment in technologies such as data immutability. We recommend the following amendment: Article 25.4: "In addition to the requirements referred to in paragraph 1, trading venues shall ensure that its ICT business continuity arrangements allow trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any IT service of the trading venue after a disruptive incident is MINIMISED" (while deleting the phrase "close to zero").

Regarding Article 26.3-4, it may not always be appropriate to include members in the testing of ICT Business Continuity Plans. We recommend the inclusion of the phrase "where applicable", similar to the formula in Article 26.2.b.

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

No

As a general comment, the industry was surprised by the level of detail and the extent of the requirements expected for the report on the risk management framework. If the ESAs maintain this level of detail and frequency, we do not believe that conducting such a review and generating a report is workable objective for financial entities. This is for two reasons.

1. As noted elsewhere in our response, the RMF is in practice composed of a range of different policies, standards and activities. These are divided among a number of teams ranging across all three lines of defence. While a financial entity may adhere to all practices listed, these will not be collected and recorded in a single document or framework. Any review will therefore involve significant coordination across many colleagues which have different reporting lines and management committees. This will make the review a complex and labour-intensive process that will require a significant number of approvals from various internal governance forums and senior managers.
2. There are several different causes for conducting the review given in Article 6(5) of DORA. If each of these causes is triggered only once in a year, which is a conservative estimate, then the frequency of the reviews would easily outpace the speed with which a financial entity could complete them. This is particularly the case given the requirement for management body review and sign-off.

We recommend the ESAs reconsider the necessity of this level of reporting and evaluate its potential impact on competent authorities as well. We believe the reporting requirements will be redundant with certain already existing reporting to the regulator by the control functions such as the results of internal audits and is therefore questionable from an added value point of view.

Further, we anticipate that such reports would be very lengthy documents that would require significant time to review. We therefore question whether the competent authorities have allocated additional resource to this task or made allowances for the time required in the existing supervisory and exam schedule. It may lead to the opposite effect, overwhelming competent authorities with excessive data and potentially diminishing the efficiency of their oversight.

We therefore recommend that the ESAs consider shifting to a single review of the RMF that accounts for the activities of the preceding year in the areas in Art 6(5) of DORA. Anything more is likely to result in a material diversion of resources from existing governance and risk management, without adding any value to the financial entities own risk management practices.

Q27 – Q32

Not answered since the question is related to Simplified ICT RMF which has been kept out of scope.

Contacts: digital@abbl.lu