European Association of CCP Clearing Houses

EACH Response to the ESAs' consultation paper on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies

September 2023

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 19 members from 15 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback to the consultation paper on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554[1].

Questions

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.

EACH is of the opinion that, in general, it is **not clear what Article 29 defines in terms of proportionality**.

Notably, the uniform application of the proportionality principle encounters challenges due to mandated obligations – such as the comprehensive testing of critical function ICT systems, broad implementation of data encryption measures, and the registration of details pertaining to all ICT services. As a proposition, it is **advisable to ensure a consistent application of the proportionality principle within DORA with clearly defined thresholds**.

Further, when considering which financial entities could become subject to more advanced testing, both the **principles of proportionality and subsidiarity should be considered**, as well as the **need to ensure a level playing field**. It would not be proportional to make all financial entities subject to the same levels of requirements without distinguishing between their levels of size, type, and criticality to EU markets. Nevertheless, the size of a financial entity should not be the most relevant metric when determining what cybersecurity requirements ought to apply. Rather, **entities should be subject to similar requirements, if they have similar risk profiles, including their systemic impact, and whether they conduct similar activities**.

In general, we would **caution against overly prescriptive technological measures which would rapidly be outdated** due to technological evolution. While there is a need for a

[1] https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTSs_ICT_risk_management_tools_methods_processes_and_policies.pdf

coordinated approach to cyber-resilience, when considering further regulatory requirements in this space it is important that flexible innovation is safeguarded since "one size does not fit all". Hence a **risk-based and proportionate approach is needed**.

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

In relation to the tasks of the Control Function under Article 2(f), we believe that the **development of security awareness programmes** and digital operational resilience training should not necessarily sit with the Control Function but instead with **appropriately skilled personnel**. We kindly suggest that the control function should instead be tasked with the oversight and monitoring of security awareness programmes.

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

We would like to kindly put forward the following considerations and suggestions:

- **Article 3** mentions **risk tolerance levels**, but it is **not clear or defined if the expected risk tolerance is determined specifically for each of ICT risk or for all of them together**. This would require clarification, as calculating the likelihood and impact of vulnerabilities and threats does not add value if it is done at the risk level.
- We consider that qualitative and quantitative indicators are not always possible to establish and therefore would like to propose to **reword Article 3(1b)** by stating that the ICT risk management policy and procedures shall include *"the procedure and the methodology to conduct the ICT risk assessment, identifying vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions and the quantitative or qualitative indicators**, if possible,** to measure impact and likelihood of occurrence of those vulnerabilities and threats*".
- We suggest **rewording Article 3(1d)(iv)** as follows: *"provisions on the review of the accepted residual ICT risk at least once a year, including the identification of **~~any~~ relevant** changes to the residual ICT risk, the assessment of available mitigation measures and the assessment of whether the reasons justifying the acceptance of residual ICT risk are still valid and applicable"*.
- We suggest **adding point (v) to Article 3(1d)** as follows: ***"monitoring that the aggregation of accepted risks is within the risk appetite of the financial entity"***. ,
- Similatly as for Article 3(1d)(iv), in **Article 3(1e)**, we would like to emphasize the importance of **closely monitoring "relevant" or "significant" aspects** that may have a material impact on the overall ICT risk profile to ensure an effective and focused approach on the critical aspects for the financial industry as well as for the regulators. **Including provisions on the monitoring of "any" changes as described in Article 3(1e) would dilute the scope and focus**.
- **Article 3(3) appears too broadly defined for implementation on the financial entity's side** in order to allow for a better understanding. We propose to **define**

specific guidelines on how to tailor and update the **ICT risk management policies and procedures** as well as **risk assessment in case of material changes** as stated in the proposal

Further, any proposed security risk management framework should, in our opinion, be based on **already existing internationally developed standards**, and any requirement to **disclose** details on cyber resilience should be conducted in a **careful manner** to ensure sharing of such information does not unintentionally better equip potential attackers, thereby increasing cyber resilience-related risk.

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

We consider that **Article 4** of the proposed RTS requires further clarification, as **its intention seems to lack clarity**. It implies that the policy should distinguish between various types of ICT third-party service providers. Yet, it doesn't elaborate on the purpose of such differentiation. The proposed wording suggests a preference for certain ICT third-party service providers over others, a determination that falls outside the RTS scope. We hence kindly **recommend its removal**.

While welcoming the definition of 'ICT asset'[2] in DORA Article 3, EACH Members would appreciate receiving **more detailed definitions of 'ICT' and 'information asset'.** The provided definition of 'information asset' in DORA Article 3 is as follows: *"'information asset' means a collection of information, either tangible or intangible, that is worth protecting".*
However, this definition could be interpreted in a way that information assets may include, for instance, databases, data files, contracts and agreements, system documentation, user manuals, training materials, operational/support procedure, business continuity plans, back up plans, audit trails, archived information.

We therefore consider the definition of 'information asset' to be imprecise and excessively broad. We therefore suggest:

1. **narrowing down the definition of 'information asset' and providing a list of examples**;
2. **providing a criticality assessment of information assets and ICT assets supporting business functions.**

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?

We consider that **both dates are equally important** as they serve different purposes e.g. "end of support dates" is being considered important, as it would enable financial entities to plan the renewal/decommissioning of underlying assets accordingly. It additionally would lead

[2] 'ICT asset' means a software or hardware asset in the network and information systems used by the financial entity;

financial entities to consider that there are assets with long procurement lead times or high costs.

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

While the suggested approach on encryption and cryptography considered in the proposed RTS is mostly in line with our view, we believe it could be **further improved** by recommending that **lost, compromised, or damaged keys shall be replaced instead of relying on recovery**, as proposed in **Article 7 (3**), as those keys are overly risky to be recovered.

Furthermore, we see a **need for clarity in Article 7 (4)**, to further specify whether the register pertains to only certificates or encompasses keys as well. We believe that **these refinements would strengthen the overall framework**, ensuring a more robust and secure approach to encryption and cryptographic key management. Too detailed descriptions should be avoided, but rather left to the entities decision based on their risk analysis in such cases.

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

EACH is of the opinion that **Article 10(2c) is excessively broad**, in particular when it comes to the reference to "vulnerabilities". We suggest **providing a clearer definition of vulnerability**, e.g. as any which would result in a critical third-party ICT service no longer being available to the customer and this impacting the customer.

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

We also consider that, in order to avoid unnecessary administrative overhead, the proposed RTS should provide more optionality on how financial institutions should organise their policies, rather than being very prescriptive on what each policy or procedure should contain. **Article 11(2f)**, on the use of "*centralized management solution to remotely wipe the endpoint device [...]"* **is very prescriptive, and likely restrictive of other solutions that may achieve the same objective**. Instead, we **recommend to list the principle that firms should have the means to remove corporate data from mobile devices**. This for example could be achieved by using containerization solutions, which doesn't require to "remotely manage the endpoint devices". Being prescriptive, risks the situation where certain solutions could be excluded, such as BYOD.

Moreover, the **synchronization of clocks requirement**, encompassed in the logging procedures proposed in **Article 12**, should be **limited and tailored exclusively to ICT**

systems serving important and/or critical services. By adopting this focused approach, it could be ensured that critical operations receive precise focus and timestamping while optimizing resource allocation across the organization and thus ensuring financial stability.

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.

The **frequency of such testing** should not be set by the supervisors within the Level 2 instruments but **determined by each financial entity within their policies using a risk-based approach**, and primarily looking at exposure to external (internet) threats. There might be measures which detect on weekly basis but depends on the ICT assets. It should be determined taking their classification, risk profile and the purpose of ICT assets as opposed to not taking into consideration especially for larger organizations. Weekly cycle is excessive for systems which are not externally exposed, because of the volume of scanning required (significantly more assets) vis-à-vis the benefits, and the fact that the overhead of doing the scanning process is significant because of change management processes required to manage scanning cycles.

Given that the number of assets is high, **running scans on "all assets" without proper consideration of the asset classification** might **impact financial entities** by causing network slowdowns. Moreover, it would also lead to a **significant number of false positives** that would need to be analyzed by the operating teams.

We therefore propose a **weekly cycle for internet facing systems and a monthly cycle for internal systems**. As a comparison CFTC Systems Safeguard Testing Regulation requires quarterly internal and external scanning cadence.

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.

Article 11(k)(i) on the requirement for the *"individual in charge of using cloud client interface to manage cloud computing resource [...]"* is unusually **prescriptive and specific**, and we propose to **remove it altogether**. This should be covered by other statement of having human resources properly trained and competent (not just for cloud security).

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

Article 13(1i) appears too vague. Any activities to identify potential vulnerabilities in network security should be covered in the digital resilience testing within DORA Level1 or specific separate RTS. We also suggest **inserting another sentence which would emphasize on**

certain exemptions being possible with regards to communication within the same data center.

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

EACH does **not support the specific approach proposed for CCPs as described in paragraph 2.3.2 of the proposed RTS and subsequent proposals**. In our view, this approach presents issues and creates undue uncertainty. It is worth notice that:

- ICT systems security is subject to intensive and extensive multilevel regulation, which includes EU and national regulations and international standards and guidelines;
- financial market infrastructures are already subject to extensive entity-specific risk management provisions, including ICT requirements. This is mainly due to the fact that vertical entity-specific regulation takes a functional approach that looks at the overall operational risk to which a specific service is exposed.

Instead, it is worth to underline that **DORA overcomes the functional approach with the aim to consolidate and upgrade ICT risk requirements to a single horizontal framework** applicable across the entire financial sector alongside the operational risk requirements that have, up to this point, been addressed separately in various Union legal acts. In this regard, we **support the centralisation and primacy of DORA**, and call of a **repeal of redundant/ equivalent ICT risk management requirements set forth in Level 2** vertical specific regulations.

In this regard, a proposal as the one supported put forward in the proposed RTS and which introduces a further specific provisions at Level 2 for CCPs appears to be **in contrast with the above mentioned objective of DORA, in particular for the horizontal approach across the financial sector for the ICT risk requirements**. Indeed, the proposed approach for CCPs introduces a differentiation between the different financial entities with the consequence that the goal of consolidation remains only at the formal level and not at the substantial level. In this regard we notice that DORA Level 1 measure includes some specific requirements for CCPs but this approach should not be replicated in Level 2.

In addition the proposed approach increase uncertainty. The proposed RTS do **not clarify how the coordination between DORA Level 2 and EMIR Level 2 will be carried out** and we are concerned about the **risk of redundancies and inconsistencies**. We believe this uncertainty undermines one of the key objectives of the DORA Level 1 as stated under recital 102 and 103, i.e. the consolidation of the ICT risk management provisions across multiple regulations and directives applicable across the financial sector.

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

We are of the opinion that, regarding, A**rticle 18(2)(d) further clarification is needed on what is meant by a "clear screen policy"**.

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

The **requirement for training is considered too prescriptive** with respect to content and frequency to be conducted "at least yearly". We kindly recommend that the **content and regularity of training is set by the organization based upon the position held, access to data and resources**, with greater flexibility for financial entities in tailoring the training content. It seems too restrictive to sum up the necessary ingredients.

Based on the above consideration, we recommend **amending Article 19(1)** as follows: *"Financial entities shall include in specific ICT security awareness programmes and digital operational resilience training elements regarding the **high-risk topics in the individual branch and organisation,** [...]".*

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.

With regards to the proposed approach on access control, we suggest including the terms **"user reconciliation" and "user recertification" as part of Article 22(e)(iv)**.

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.

Concerning **Article 24(5)**, EACH Members consider that the **listed criteria** to trigger ICT-related incident detection and response processes seem to be excessively constraining, **potentially leading to identify every incident at major**. We would therefore call for a **more proportionate set of criteria**, clarifying that **only security-related incidents are being targeted in this context**, in line with DORA Article 3a which defines an ICT-related incident as *"a single event or a series of linked events unplanned by the financial entity that compromises the **security** of the network and information systems".*

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

Concerning **Article 26(6)**, we suggest specifying that the **review of business continuity plans** mandated on a yearly basis only apply to those business continuity plans **related to critical functions.**

Moreover, we consider that in **Article 26(3)** there should **not be for CCPs a mandatory and prescriptive requirement to include in BCP testing *"clearing members, external providers and financial infrastructure"***, as it is excessive and overly burdensome for CCP

operational teams. The decision to include some external stakeholders should be **risk-based and proportionate**.

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

We consider that a **one-size-fits-all model for duration and recovery would not be suitable**. Moreover, any regulatory measures in this space would need to be sufficiently broad to allow flexibility to new types of situations and issues, recommending specific and quantitative parameters should thus be avoided. It is very important that different approaches, in line with the different needs are allowed.

On a general basis, **financial market infrastructure operates under a two-hours RTO guidance**, as per CPMI-IOSCO Principles of Financial Market Infrastructure[3]. Two-hours RTO guidance works well under operational disaster recovery plans, but we consider that mandating RTO under specific legislation would be counterproductive.

In addition, **Article 25 section (2c)(iv)**, opens the possibility for having the third (or even fourth) processing site. We propose **removing this paragraph** focusing on having the **secondary processing site with the correct risk profile** to ensure continuous operations when the primary site fails.

Article 27(2) lists scenarios and mandates including all those scenarios in response and recovery plans. We **respectfully disagree with this approach**, finding it prescriptive on specific scenarios because the list cannot be comprehensive and all encompassing. Instead, we **recommend adopting an "all hazard" approach** on planning and testing based on the **impact of an event**, such as loss of workspace, technology staff, etc., regardless of the scenarios that may have caused the impact.

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.

We suggest **reducing the content of the report on the ICT risk management framework review**, especially for reviews that are triggered ad-hoc by major ICT-related incidents. In this case, we would rather favour following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes.

Article 28 of the proposed RTS indirectly defines the scope of the review, as it specifies the content of the report documenting the review of the ICT risk management framework **without differentiating between different reasons for such a review** (i.e. regular review, review after a major ICT-related incident). While we consider the content of the report in accordance with Article 28 to be appropriate and reasonable in the case of an annual review,

[3] https://www.bis.org/cpmi/publ/d101a.pdf

we **miss a differentiation between the scope of the review and the content of the report in the case of major ICT-related incident**s. In our opinion, the content proposed in this Article is too broad as far as reports on major ICT-related incidents are concerned. Rather, the content of the report should be determined depending on the cause of the major ICT-related incident and should only concern the systems and services affected by the specific incident) or where there may be an impact due to interdependencies.

To summarise, we consider that:

- **The impact of the incident and the root-cause analysis should determine the scope and details**. Our rationale is the following:
    - Because of the reference to DORA Article 6(5)[4], Article 28(2) it also indirectly determine the scope of the review of the ICT risk management framework. Article 28 of the proposed RTS does not differentiate between annual reports and reports in the event of a major ICT-related incident. As a result, the scope of the report is the same in both cases, according to DORA Article 6(5), which means that the entire ICT risk management framework must be reviewed after each major ICT-related incident. This approach is too broad; in our opinion, the format and content of the report should be different in the case of the annual review and the review following the occurrence of a major ICT-related incident, since the latter would, in the rarest cases, concern the entire ICT risk management framework.
- There is **no need to analyse all services provided by the CCP, if only one service is impacted** where there are no dependencies with other services provided. There are indeed CCPs that operate two different clearing systems that are not interdependent, and we therefore do not believe it is necessary or appropriate to review the entire ICT risk management framework (i.e., all systems) if, for instance, a major ICT-related incident only affects only one of the services provided and the related system and has no impact on the other service and/or the other related system.

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

The **suggested approach** regarding ICT business continuity management under the simplified ICT risk management framework appears **sufficiently substantiated**.

[4] 5. *The ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request*