Contribution ID: ad06a4a0-bdaa-4c05-8a3f-d8c74a9baed4
Date: 11/09/2023 17:39:51

Consultation 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

Fields marked with * are mandatory.

Introduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the first batch of Consultation Papers on the mandates stemming from the Digital Operational Resilience Act (DORA) with the aim to collect market participants' feedback on the proposed draft regulatory technical standards (RTS) to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554.

Market participants are invited to provide their feedback to the draft technical standards by responding to the questions presented in this consultation paper. The feedback received will be taken into account in the finalisation of the draft technical standards, which are due to be submitted to the European Commission by 17 January 2024.

Comments are most helpful if they:

- respond to the questions stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence (including relevant data, where applicable) to support the views expressed;
- reflect a cross-sectoral (banking, insurance, markets and securities) approach, to the extent possible; and
- describe any alternative approaches the ESAs could consider.

To submit your comments, please click on the blue "Submit" button in the last part of the present survey. Please note that **comments submitted after 11 September 2023 or submitted via** other **means may not be processed.**

Please clearly express in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from the ESAs in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request.

Any decision we make not to disclose the response is reviewable by the ESAs' Boards of Appeal and the European Ombudsman.

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the ESA websites.

General Information

* Name of the Reporting Stakeholder

Electronic Money Association

Legal Entity Identifier (if available)

* Type of Reporting Organisation

☐ ICT Third-Party Service Provider
☐ Financial entity
☑ Industry Association/Federation
☐ Consumer Protection Association
☐ Competent Authority
☐ Other

* Financial Sector

☑ Banking and payments
☐ Insurance
☐ Markets and securities
☐ Other

* Jurisdiction of Establishment

Belgium

* Geographical Scope of Business

○ EU domestic
○ EU cross-border
○ Third-country
● Worldwide (EU + third-country)

Name of Point of Contact

Judith Crawford

* Email Address of Point of Contact

judith.crawford@e-ma.org

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.

We support the adoption of a proportionate and risk-based approach by the ESAs in specifying elements of the ICT security/business continuity management frameworks that are listed in Article 15 of DORA. The scope of controls that are detailed in these frameworks should reflect the size and complexity of the regulated entities and of the services they provide.

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.

Further harmonisation of ICT risk management tools, methods, processes and policies (Article 15)

ICT security policies, procedures, protocols and tools

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

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

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

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 important that firms track the end date(s) for the support provided by providers and manufacturers of ICT assets that directly support the delivery of Critical/Important business functions. We also want to highlight that we perceive that it will be very difficult for firms to identify (i) All ICT assets that are used by chain supply service providers (chain outsourcers) to support the delivery of such functions (ii) Associated support end dates for such chain outsourcers' ICT assets. This task becomes even more complicated due to the extended supply chains used by firms involving n-th party service providers (4th, 5th, ….) that are often invisible to the regulated firm or to its direct outsourcers. We propose that firms are only required to track and record support end dates for ICT assets supporting the delivery of Critical business functions that are provided by 3rd party outsourcers (external, intra/inter-group) and by their direct sub-outsourcers (4th party providers).

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

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.

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

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.

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.

Many financial service providers already perform automated vulnerability scans on an ongoing basis to comply with industry information security frameworks (ISO 27000, PCI-DSS). The target(s) and frequency of execution of such scans are determined by the risk profile of underlying ICT assets and their role in supporting the delivery of specific services. A blanket requirement to carry out automated vulnerability scans of all ICT assets would extend the testing resources of many firms for limited returns. The benefits of the adoption of such a blanket approach will also be limited by limitations in the ability of firms to review and reconcile false positives generated by automated scans. Therefore, we encourage the ESAs to allow firms to continue to carry out regular vulnerability assessments focusing on Critical ICT assets.

We would also encourage the ESAs to afford flexibility to firms to decide on the frequency of these vulnerability scans to reflect the underlying risk profile of the ICT asset and the company risk appetite. We perceive this to be a more effective approach rather than the adoption of a prescriptive 1-week frequency of scanning.

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.

We would encourage the ESAs to consider the use of logging arrangements (outlined in Art.12 of the RTS) to record interactions of users/systems with cloud resources over authorised cloud resource access interfaces

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

We are concerned that the requirement introduced in Art.13 (c) of the draft RTS to “use a separate and dedicated network for the administration of ICT assets” is overly restrictive and would yield limited network security benefits. We encourage the ESAs to remove this text from Art 13 (c).

Here, we note that Art.13 (a) of the RTS already requires the use of segregation and segmentation of ICT systems and networks based on their criticality.

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.

Q15: Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

We would encourage the ESAs to provide further clarity on the requirement introduced in Art. 17 (2) (b) of the draft RTS.

We note that it is common practice to involve the entities that require and develop changes to ICT assets in the change review and final approval process. After all, they often represent the end-user and technical subject matter expert (SME) communities. We also acknowledge the importance of ensuring the involvement of additional, independent stakeholders (Cybersecurity, Product Ops/Admin, CTO) in the change review /approval process.

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.

We perceive that the dynamic of existing outsourcer relationships limits the ability of financial service providers to seek access to the ICT project/change management policies of large, Critical outsourcers. The CTTP Overseer that is introduced in DORA may be able to receive access to the relevant policies of such outsourcers and assess alignment against good financial services' industry practice.

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

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

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.

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

Human resources policy and access control

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.

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.

ICT-related incident detection and response

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.

ICT business continuity management

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

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

Report on the ICT risk management framework review

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.

Simplified ICT risk management framework

Simplified ICT risk management framework

Q27: Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.

Further elements of systems, protocols, and tools to minimise the impact of ICT risk

Q28: Do you agree with the suggested approach regarding the further elements of systems, protocols, and tools to minimise the impact of ICT risk under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

Q29: What would be the impact for financial entities to expand the ICT operation security requirements for all ICT assets? Please provide details and if possible, quantitative data.

Q30: Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples.

ICT business continuity management

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.

Report on the ICT risk management framework review

Q32: Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.

Submission of the responses

Contact

Contact Form