Contribution ID: c655c4fb-2621-48a2-96f2-ad847062e7cd
Date: 11/09/2023 12:22:08

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

Dutch Federation of Pension Funds

Legal Entity Identifier (if available)

52988368

* Type of Reporting Organisation

- [ ] ICT Third-Party Service Provider
- [ ] Financial entity
- [x] Industry Association/Federation
- [ ] Consumer Protection Association
- [ ] Competent Authority
- [ ] Other

* Financial Sector

- [ ] Banking and payments
- [ ] Insurance
- [ ] Markets and securities
- [x] Other

* Jurisdiction of Establishment

The Netherlands

* Geographical Scope of Business

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

Name of Point of Contact

Martin van Rossum

* Email Address of Point of Contact

rosum@pensioenfederatie.nl

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.

The Dutch Federation of Pension Funds welcomes the opportunity to comment on the RTS on ICT Risk Management. Dutch pension funds support DORA's goals and perceive them as necessary. The EU financial sector should be resilient to digital risks, which are not limited to national borders. We therefore embrace harmonization at the EU level. At the same time, we have reservations with the effectiveness of DORA and its delegated acts. We specify our concerns from a Dutch Pension fund sector perspective.

Take the specificities of pension funds into account

We see that this horizontal financial sector regulation does not consider many of the specificities of the pension sector, by which many prescribed measures will not lead to the envisioned contribution to risk mitigation for pension funds. DORA should contribute to the ultimate goal of pension funds, which is to provide a good pension to their members and beneficiaries.

Pension funds are not typical financial market participants. They have their own specificities. If legislators wish to make horizontal legislation for the entire financial sector, they should regard the specificities of pension funds by allowing room for adapted implementation.

A vital difference between business processes of pension funds and banks, lies in their periodicity. Pension funds pay out pension entitlements once a month, whereas banks process a high volume of transactions all the time. Therefore, the impact of an ICT-related incident is substantially lower, which warrants milder control measures.

DORA should allow for sector-specific characteristics to be taken into account in the implementation by allowing a risk-based and principle-based approach to DORA requirements. It is in the interest of the European financial system to allow for a risk-based and principle-based application of DORA requirements within the pension fund sector. That would mean for financial entities to adhere to statutory principles and to define, under regulatory supervision, appropriate control measures and explain compliance with DORA. This approach is already common within the Dutch financial sector and supervised by the National Competent Authorities. Supervisory guidelines set by De Nederlandsche Bank (DNB) in its Good Practice on Information Security could be taken as a good practice.

Proportionality

Adequate requirements would avoid disproportionate and unnecessary costs on the part of pension funds and supervisors. The detail of the provisions and the lack of proportionality are reasons for our concern. Many required control measures, as currently designed, are not purposeful to enhance pension funds'

operational resilience. Instead, a large amount of control measures, applied in a rule-based fashion will disperse resources of pension providers and supervisors, rather than addressing the most serious risks.

In this vein, delegated acts should be in line with DORA Recital 21, which aims to “facilitate an efficient supervision of institutions for occupational retirement provision that is proportionate and addresses the need to reduce administrative burdens on the competent authorities”. And, “in particular, supervisory activities should focus primarily on the need to address serious risks associated with the ICT risk management of a particular entity.”

The Dutch Federation of Pension Funds thinks not enough proportionality is applied. The proportionality in the RTS for ICT Risk Management refers to a light regime for pension funds with fewer than 100 participants. There is no pension fund in the Netherlands with fewer than 100 participants. All pension funds must therefore meet all the requirements of the RTS that also apply to systemically important banks and global insurers. The operations of a pension fund cannot be compared to the operations of banks and insurers. Therefore, a real distinction must be made between pension funds and other financial institutions.

If all prescribed control measures have to be implemented without proportionate application, this will dramatically affect pension funds’ costs, which will directly reduce its members’ and beneficiaries’ pensions.

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.

As a general comment, it should be noted that a large part of the guidance provided in the different RTS and ITS consultation documents presented by the ESAs, effectively results in a translation of DORA Level I principle-based requirements into DORA Level II rule-based requirements. Furthermore, these rule-requirements are based in several instances on existing requirements for one specific category of financial institutions (e.g. banks), which means they are ill-fitting for pension funds.

In the introduction of these more stringent rule-based requirements, the proportionality principle introduced in article 4 DORA has been substantially limited. Size effectively seems to be the only remaining measure of proportionality, while the nature, scale and complexity of the services, activities and operations are no longer regarded.

As a result, many of the initial DORA requirements are translated into level II implementation requirements that are more stringent than necessary for pension funds (IORPs) and their service providers to realize an acceptable level of digital operational resilience.

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?

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

Article 6, paragraph 2(a) requires all data to be encrypted. If encryption of data in use is not possible, financial entities must process data in a separated and protected environment. Data encryption is a control measure and should be treated in accordance with a classification of availability, integrity and confidentiality, the CIA triad. For publicly available data and data that classify as low-risk, it should be possible to make the decision not to encrypt it. The draft RTS does not allow for this prudent choice. This rules-based approach thus creates disproportionately heavy risk management. At the least, an exception should be made for publicly available data and data that scores low on the CIA triad.

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.

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

Article 9, paragraph 1 obliges financial entities to identify the capacity requirements of their ICT systems and implement resource optimization and monitoring procedures. Pension provision operations, and specifically pension administration, has a high degree of plannability. This warrants a risk-based approach for pension funds in operations security. The drafted article would be disproportional.

Article 10, paragraph 2(c) obliges ICT third-party service providers to handle any vulnerability and report them to the financial entities. This would mean that every vulnerability will be transferred by all parties in the ICT chain. This is not efficient. It will create reporting overload. As most reports will be irrelevant, monitoring such reports could be seen as administrative necessity and serious vulnerabilities could be overlooked and unaddressed.

To avoid duplicate notification of incidents with the same root cause by various financial entities, it would be good if parties could refer to an incident identification number, instead of reporting the incident separately.

Article 11, paragraph 2(f) creates the same rules for private non-portable endpoint devices as for portable endpoint devices. We do not find it a realistic risk that a financial entity's core data would be wiped remotely with current measures in place preventing unauthorized deletion of data. This rule would effectively make the use of (private) endpoint devices such as laptops and phones impossible.

Article 12, paragraph 2(c) requires the logging of events related to access control, capacity management, change management, and network traffic activities. When so much information has to be logged, it produces a lot of false positives. Researching them requires a lot of man-hours, which then cannot be deployed on other essential issues. This activity risks being seen as unnecessary administration. The option to apply professional judgement would improve the adaptation of this requirement.

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.

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.

Weekly vulnerability scans for all ICT assets are already common practice with Dutch pension funds. We therefore foresee no impact of this measure.

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.

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

Article 13, paragraph 1(b) requires mapping and visual representation of all the financial entity' networks and data flows; as well as segregation and segmentation of ICT systems and networks based on their criticality, classification, and risk profile. This would require significant investments, while this information is not required for most organizations in the pension sector, due to the limited complexity of their network relative to banks and international payment processors.

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.

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

We are of the opinion that the prescribed approach on project and change management will adversely impact the implementation of more modern development approaches, such as Agile working. Additionally this will limit hiring of staff who are trained and experienced in such newer approaches.

Article 16, paragraph 4 introduces a requirement to do a source code review. We think ICT third-party providers will not want to make all source codes available to financial entities. Moreover, such a review is not the expertise of pension funds. We believe that pension funds should be able to rely on cybersecurity product quality assurances, which is in line with EU digital contract rules.

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.

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.

No.

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.

No.

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.

Article 27, paragraph 2 prescribes such an amount and specificity of scenarios to identify, that the measure will lose its value. Only scenarios that are relevant to the financial entity should be investigated. Scenarios that do not (or cannot) apply to the institution at all or whose probability is extremely low will only result in unwillingness to comply among staff, unnecessary paperwork and high costs.

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.

Article 28 is very prescriptive in formats. It would not allow pension funds to attune to the most relevant aspects for the sector. Currently used formats would no longer be allowed. That would negatively impact the helicopter view of pension fund board members.

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