Contribution ID: 2a04c64e-c187-4bd1-851e-c8806d37fce5
Date: 11/09/2023 12:25:57

Public consultation on draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554

Fields marked with * are mandatory.

Intorduction

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 Technical Standard. This Consultation paper covers:

'Draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under 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 (LEI) if available

52988368

* 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
- [x] Other

* Jurisdiction of Establishment

The Netherlands

* Geographical Scope of Business

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

* Name of Point of Contact

Martin van Rossum

* Email Address of Point of Contact

rossum@pensioenfederatie.nl

Questions

Question 1. Do you agree with the overall approach for classification of major incidents under DORA?

- ○ Yes
- ◉ No

* 1b. Please provide your reasoning and alternative approach(es) you would suggest.

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.

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.

We believe the specificities, activities and operations of institutions for occupational retirement provision (IORPs) and their service providers have not been amply taken into consideration in the approach taken. Many problems relate to the fact that IORPs outsource a significant part of their core business, such as asset management, actuarial calculations, accounting and data management, to service providers, as DORA recital 21 stipulates. Several Dutch pension fund service providers only have a handful of clients. Together, this means that almost every incident would meet the criteria of affected financial counterparts and critical services affected.

We would suggest the ESAs to consider entity-specific deviations for IORPs from criteria and thresholds in several instances. It seems that the ESAs have considered this option, but have rejected it so far.

We fear many ICT-related incidents that are not material for IORPs or other stakeholders would meet thresholds as currently specified by the ESAs. This would create a disproportionate amount of work on the part of both IORPs and supervisors on investigation and reporting the incident, which distracts efforts from a quick resolution of the incident. We consider that an ICT-related incident can only be classified as major if it either affects a service that supports a critical or important function; or if it compromises the availability, authenticity, integrity and confidentiality of data. In other words, we consider the critical services affected or data losses as a necessary criterion for classification of an ICT-related incident as major.

We do not consider Clients, financial counterparts and transactions affected to be a primary criterion. This criterion has been designed in a way that many incidents at big financial entities satisfy this criterion. The ESAs suggest an approach where an incident is classified as major when at least one primary and two secondary criteria are met. With clients, financial counterparts and transactions affected as a primary

criterion, that means many incidents that are not material to the financial entity or it clients will nevertheless be reported as major, creating ‘false positive’ reports that also require processing by the supervisor.

We appreciate that the ESAs develop an established set of criteria for incident classification. This is in line with SOC II and ISO 27001 standards. Looking at good market practices implementing these standards, we note that criteria for incident classification tend to regard the materiality of their impact. That is not the case for clients, financial counterparts and transactions affected.

The ESA’s chosen approach depreciates the concept of major ICT-related incidents and will potentially lead to a less vigilant security approach at IORPs. It will also create disproportionate reporting burdens for financial entities as well as disproportionate work for supervisors to assess and process incident reporting. Important incidents risk being subsumed by irrelevant ones. Operational resilience is not attained effectively by classifying large incidents as major, without regard to their impact. We would suggest to make clients, financial counterparts and transactions affected a secondary criterion. We see no need to adjust the conditions for classifying incidents as major accordingly.

We are glad that reputational impact has been assigned as a secondary criterion. Reputational damage cannot be measured well. This concerns both the unit of measurement and the time period after which the damage would be undone. Even if an incident gets media attention, that does not necessarily give a factual view of the impact on the organization and its customers. This is evidenced by the lack of public attention in news reports on disruptions in digital payment systems. Temporary disruption in payments systems are nowadays more considered ‘facts of life’ than ten years ago.

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?

- ○ Yes
- ◉ No

* 2b. Please provide your reasoning and suggested changes.

We are deeply concerned that with the current specifications and thresholds, most incidents will undeservingly trigger this criterion for many pension funds.

DORA Recital 21 states that competent authorities should “maintain a vigilant but proportionate approach in relation to the supervision of institutions for occupational retirement provision” which, “outsource a significant part of their core business, such as asset management, actuarial calculations, accounting and data management, to service providers.” This close relationship should be reflected in the application of delegated acts.

Many such service providers only provide services to one or a limited number of legal entities. They can be affiliated or intra-group, but this is not the case everywhere. That means that several big service providers only have a handful of financial counterparts. In the case of asset managers, they fall in scope of the DORA. In many instances, the ICT-infrastructure and processes are the same for each respective client. That means that most ICT-related incidents will trigger the conditions of affecting 10% of all financial counterparts. This seems disproportionate. We would propose that, additionally to the relative criterion of 10% of all financial counterparts affected, an absolute criterion of at least 20 financial counterparts affected should be satisfied.

The ESAs suggest separating conditions for clients, financial counterparties and transactions. Meeting any of these conditions will trigger this criterion. In our view, that sets the bar far lower than the (co-)legislators have intended. We consider it disproportionally easy to trigger this criterion. We suggest making the triggering of the criterion conditional to meeting a combination of at least two triggers covering at least two of the aspects of this criterion.

With regards to impact on relevant clients or financial counterparts, we refer to recital 21 in DORA, which stipulates that IORPs outsource a significant part of their core business, such as asset management, actuarial calculations, accounting and data management, to service providers. This criterion leads us to believe that this criterion should not apply to the pension fund’s service provider. The service provider’s business is so crucial to the pension fund that any incident would affect the implementation of the business objectives of the pension fund.

It should be understood that many pension service providers provide a standard service to a limited number of pension funds. Pension funds are rather simple organizations that usually execute a single product /service – the pension scheme – to all of it members and beneficiaries. That means that the absolute and relative thresholds for clients affected will be affected just as well.

Another suggestion for this criterion would be to introduce a consolidated approach, whereby the pension fund and its service provider are considered as one. This would recognize the strong bond between pension fund and service provider and as does justice to DORA Recital 21. The criterion Clients, financial counterparts and transactions affected would be applied to the pension fund as a the end client of the service provider. The consolidated approach could be structured as a counter evidence, whereby the pension fund and its service provider can only apply this approach if they can substantiate its effectiveness.

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?

- ○ Yes
- ◉ No

* 3b. Please provide your reasoning and suggested changes.

Duration and service downtime
The ESAs note that since this threshold will apply to IORPs, which have not yet been subject to incident reporting requirements prior to DORA, feedback from market participants will be welcomed on whether the 2-hour service downtime threshold is appropriate for their business. We are happy to provide insights from the view of IORPs.

A vital characteristic of pension funds is the periodicity of their activities. Pension funds pay out pension entitlements once a month. Administration and transaction systems are effectively only active on certain days of the month. We believe service downtime should only be understood as those hours in which systems supporting critical or important function are being used; or are 'online'. If a service does not need to be 'on', it does not make sense to consider it 'down'.

Outside of the hours where systems supporting critical or important functioning are used, incident duration should not be seen as service downtime. The availability, authenticity, integrity and confidentiality of pension data are then still at stake, but these aspects are already covered in the criterion of data losses.

When looking at the duration of an incident (art. 3.1), a proper definition of the word 'resolved' seems to be missing. Adequate knowledge about the progression of an incident and its resolution(s) is essential to the determination of the duration of an incident. Because of this, we propose to apply the same 'end' criterion as for the termination of service downtime, "the moment when regular activities/operations have been restored to the level of service that was provided prior to the incident".

IORPs' activities are commonly divided between asset management and pension administration services. Within pension administration, we only consider collecting pension contributions, payment of pension benefits and updates of pension entitlements as supporting critical functions and therefore relevant for the purpose of this criterion. These services are only active certain days of the month. Any incidents affecting these services outside of these active hours should only trigger the criterion duration and incident downtime if its duration is at least 24 hours.

Regarding service downtime in asset management services, essential functions are limited to trade repositories and the administration of other financial transactions; integrated investment management systems, client relation management systems and the hosting of these systems. The 2-hour service downtime threshold for incident reporting in trade repositories could also be applicable to other trade administration systems.

Further asset management systems include customer relation management systems for administrative support, reporting systems, transaction processing systems, financial data systems and order management systems for financial trades. These services are in turn supported by (web) hosting services. To determine which systems support critical or important functions, we suggest to follow existing national guidance and regulation on outsourcing for pension funds.

Reputational impact
We believe for reputational impact to be used in the classification of ICT-related incident, the specifications of the proposed criterion need to be limited. If an incident gets media attention, that does not necessarily give a factual view of the impact on the organization and its customers. It could be taken into account to flag the potential impact of an incident, but not as impact of and by itself.

It seems appropriate to remove this specification, so that reputational damage is measured in terms of its

impact on complaints, meeting regulatory requirements and/or losing clients or financial counterparts. Furthermore, additional functional thresholds should be created to be able to adequately measure the level of visibility of an incident within the market. That way, the criterion would be triggered only if there is demonstrable reputational impact.

Economic impact
We suggest major ICT-related incidents should involve at least €1 million in material damage.

Staff costs are difficult to calculate. Resolving ICT-related incidents is part of ongoing activities. If an incident occurs at a quiet time, no additional staff needs to be involved. In such case, there is no direct loss in staff costs. Only if an incident incurs additional staff costs on top of the budget, costs would have to be attributed to the cost of the ICT-related incident.

Question 4. Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13?

- ○ Yes
- ○ No

Question 5. Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14?

- ○ Yes
- ◉ No

* 5b. Please provide your reasoning and suggested changes.

We think this criterion is too broadly formulated. In our view, the specification of whether an incident has affected services or activities that require authorization is not relevant enough to feature in this criterion. Many services require authorization, It seems therefore that this specification touches upon the authenticity, integrity and/or confidentiality of data, which is already covered in the criterion 'data losses'. It is not appropriate for this specification to feature in two criteria, thereby triggering two primary criteria at once.

An assessment of whether the incident has affected ICT services that support critical or important functions of the financial entity should be enough.

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?

- ○ Yes
- ○ No

Question 7. Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17?

- ○ Yes
- ○ No

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?

- Yes
- No

Contact

Contact Form