PensionsEurope answers to the consultation of the ESAs on DORA second batch of policy products

March 2024

www.pensionseurope.eu

1 PensionsEurope answer regarding the ESA's consultation on Draft RTS and ITS on major incident reporting

Question 1: Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes. (**No**)

PensionsEurope welcomes the European Union's commitment to establishing a digital operational resilience framework for the financial sector and recognises the importance of protecting digital infrastructures from cyber threats.

We note that no proportionality is given concerning timelines for reporting. That does no justice to the size or risk of different types of financial entities. We urge ESAs to explore the idea of different timelines depending on the type of financial entity, to better capture the specificities of the different types of financial entities such as IORPs which are not operating on a 24-hour a-day and 7 days a week basis like in the payment sector but rather on a monthly cycle. Level 1 of DORA (article 20, (a) iii) outlines: "*take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations,* ***and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, specificities of financial sectors****, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to this Regulation and to Directive (EU) 2022/2555*".

Furthermore, we acknowledge the need to tackle major incidents, but we would like to understand if it is feasible for national competent authorities to act in such cases and if that justifies the short timeline for the initial notification.

The proposed time limit for the initial notification is not suitable considering the following points:

1) The very complex architecture of the criteria to classify an incident as major, which requires obtaining a lot of information from a lot of different sources within the entity, in several Member States and the media. Despite some simplifications brought in the final report sent to the Commission on 17 January 2024, the classification of major incidents remains time-consuming.

2) Timeline is too challenging for situations where an incident relates to multiple financial entities, as each party will need to gather information from the financial entity or third party at which the incident was initiated. This may strain (answering, replying, and discussing) the crisis response for the incident and may result in reporting delays. The team, usually accountable for the classification and the reporting itself does not work 24/7. This organizational issue will be even greater for SMEs.

3) Brief deadlines may result in premature notifications of significant incidents, necessitating later reclassification as non-major. Incorrect classifications based on an incomplete analysis or poor-quality data

would entail administrative correction afterward, which would create unnecessary administrative burdens, both for the financial entities and for the authorities.

4) The pensions sector is different from payment services. Indeed, the 4-hour timeline is aligned with PSD2 but does not fit with the pension and insurance sector. Thus, the pensions sector does not have functions that are critical on a 4-hour basis or even on a 24-hour basis. In this regard, it must be stressed that as indicated above, that level 1 of DORA encourages the ESAs to provide different timeframes for different sectors.

Therefore, to extend our argumentation, we would propose to mirror the 72-hour deadline in the GDPR legislation to ensure consistency across the regulation. In that case, it would mean that financial entities would have no later than 72 hours from the detection of the incident to submit the initial notification.

As for the timelines for intermediate reports, we are also concerned. Thus, considering the overwhelming amount of information that the financial entities are requested to provide to the authorities, the proposed 72-hour deadline for submitting intermediate reports is too short. Consequently, either the amount of data that needs to be provided to the authorities must be limited in scope or the deadline needs to be longer.

We are worried that the timeframes might be too brief when an incident involves multiple financial entities. The organization where the incident originates will be overwhelmed by requests from financial entities that all take their own approach and information requirements, generating excessive administrative expenses. Uniform reporting and extended deadlines are needed in such cases.

The deadline for initial notification could also be prolonged in cases where the incident originates with a (sub-)contractor. Timelines are too short to request and process data from third parties. The amount of data that needs to be provided must be limited and deadlines extended. The third-party or sub-contractor could be allowed to report to the supervisor directly on behalf of the financial entity. Financial entities should be able to reasonably depend on those reports to a certain extent.

As to Article 6(2), we would like to point out that the wording “within one hour following regular starting time of the next working day” is impractical since IORPs have no uniform working time schedules. We suggest replacing it with “by noon local time for the reporting entity”.

Finally, a counterproductive incentive is given to delay the classification of an incident as major. Considering that the initial report should be filed within 4 hours after the classification and within 24 hours from the time of detection of the incident, financial entities would have an incentive to classify the incident as major only after 20 hours, to have the maximum amount of time for the initial notification. It seems best to drop the reference to a certain number of hours after classification as major.

Question 2: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes. (**No**)

ESAs drafting should be consistent with EC willingness to streamline reporting requirements in line with the political goal of reducing them by 25%, as outlined by the EC president, Ursula von der Leyen during her State of the Union speech on 13 September 2023. A minimalistic approach is preferred for the initial notification to focus attention to incident resolution and avoid supervisors from being overwhelmed.

The number of data fields as prescribed by the draft RTS would be burdensome for financial entities, especially for IORPs which are often small size organisation and have few human resources. While the ESAs indicate that having less than half of mandatory data fields on the total of data fields gives flexibility for financial entities, we believe that this does not take into consideration the specificities of IORPs which are often not-for-profit organisations, embedded in social and national contexts.

Therefore, we encourage ESAs to reduce the number of proposed data fields in the DORA incident reporting template. The large amount of data fields will mean that financial entities will rush to obtain information from various departments, without time to assess this information, which would not lead to a consistent approach to the reporting. It will be also difficult for NCAs to assess the reporting being produced. Furthermore, some of the requested information is already within the knowledge of the NCAs, such as the organization's name, its Legal entity identifier, and the contact persons.

The number of questions for an initial notification is extensive and may negatively impact the timeline of notification.

Questions 2.9 and 2.10 lack precision and may not yield accurate factual information. It should be considered to specify these questions more. The financial entity might not have good insight into the direct impacts of incidents on other financial entities and third-party providers, and vice versa.

The question regarding recurring incidents (2.11-13) may likely be more appropriate for the intermediate report as this information may not be available within the first four hours and requires analysis and input from IT staff mitigating the Incident. Hence, unless it's clear that an incident is recurrent, it's counterproductive to dedicate time to assess its recurrence during the initial or intermediate phases of incident response. Therefore, we suggest making data field 2.12 mandatory only for the final report.

Question 2.15 will not result in relevant information without detailed knowledge of how the business continuity plan in question is structured. Therefore, we suggest removing this question. Lastly, question 2.16 asks for 'Other information'. This can be anything and may result in discussions at the financial entities, and perhaps spending resources to provide this information that could be better spent in resolving the incident. Instead, we find it more appropriate for the supervisor to request more specific additional information later in the process.

Furthermore, reporting the information would be best through an online platform. The means of reporting is not clear in the current draft RTS.

Considering the 24-hour deadline for submitting the initial notification from the time of detection of the incident, it is unrealistic to expect that the financial entities can perform an adequate analysis to determine whether the thresholds for the criteria that can trigger a major incident have been met (cf. data field 2.4).

Question 3: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes. (**No**)

As indicated earlier, ESAs drafting should be consistent with EC willingness to streamline reporting requirements in line with the political goal of reducing them by 25%, as outlined by the EC president, Ursula von der Leyen during her State of the Union speech on 13 September 2023.

As for our answer to question 2, we also encourage ESAs to reduce the number of proposed data fields, to reduce the number of data fields in the intermediate report. Considering the complex design of the classification criteria to classify an ICT incident as major, it would be also difficult for financial entities such as IORPs to collect information from different sources within the entity. We question the added value to report information in such a short time. We consider that the required information may not be of great added value in the spirit of this process.

Additionally, and perhaps more significantly, gathering the information for the intermediate report can take a lot of capacity and resources. It may be considered that major incidents are very irregular and the ways to gather and assess the needed information are not a standard procedure for the financial entity. This may result in significant effort and use of resources to assess (under time constraints) ways to gather and report, resulting in a larger than-needed resource claim and cost to resolve the incident. This may mean that these activities are included in the Business Continuity Plan, without direct impact on resolving the incident at hand. We suggest considering the need for this information considering the purpose of the process.

For example, Article 4 (b) "Date and time of occurrence of the incident" of the draft RTS is concerning. Thus, the occurrence of an incident might require forensic analysis, and therefore it may not be identified before the intermediate report is required to be submitted. Therefore, we would propose to move Article 4 (b) to the final reports section (article 5). Data fields asking for descriptions (3.21, 3.23, and 3.37) are suggestive and may not result in quantifiable data. Such reporting should be avoided.

In continuation hereof, the ESAs should go through the individual data fields to further evaluate whether the requested data is strictly necessary for the authorities to perform their tasks.

Finally, there is also an inconsistency when it comes to the voluntary notification of significant cyber threats, ESAs note that *"in order to encourage the reporting of such threats, the reporting template should not pose any burden to FEs to prepare and submit to CAs"* (page 12, point 25), but that logic is not applied to the mandatory reports. We strongly urge the ESAs to apply similar reasoning to mandatory reporting, to ensure a smoother implementation of the draft RTS.

Question 4: Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes. (**No**)

While the information requested in the final report seems more acceptable, given the reporting timeframe, **we would encourage ESAs to assess those data fields against the background of the data fields required under the whole DORA incident reporting template which is likely to overwhelm national competent authorities.** A review of the cost-benefit analysis for the data fields could lead ESAs to keep those strictly necessary to carry out the tasks conferred on ESAs.

Analyzing the cost and loss breakdown in data fields 4.14 to 4.25 will be particularly laborious and time-intensive. Certain expenses, such as those related to customer redress and compensation (4.19) and fees

resulting from non-compliance with contractual obligations (4.18), may not accrue within a month, thus rendering the data unavailable.

Since major incidents are likely rare, the reporting of staff costs (4.17) needs to be implemented ad hoc when an incident occurs. Reporting is only mandatory 'when applicable', though in practice there will always be staff costs involved. Instead, reporting on staff costs should be voluntary.

Resolution of an incident is likely considered a 'run' activity that requires no separate recording of hours spent. This may lead to frustration among staff about adhering to such an ad hoc procedure with no direct impact on the resolution of the incident. It may also be considered that it is resource-intensive to organize during a period of crisis. This may result in another addition to the Business Continuity Plan with no direct impact on restoring a critical process or system and potentially claiming resources needed to resolve the incident. The necessity of this information should be reconsidered considering the purpose of the incident resolution process. We suggest more space should be given to provide estimates and to report in less detail, to limit the required overhead for this process.

Question 5: Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes. (**Yes**)

We agree on the proposed data fields, although we would like to suggest changing some fields from "mandatory" to "optional". The most important is that the threat is reported as early as possible. The time required to report a threat is proportional to the number of mandatory data fields and this could be due to some internal difficulties in reporting a threat. Our suggestion is to change the classification of data fields 10, 11, 12, and 18 from "yes" to "optional"; and of data fields 19 and 20 from "yes, if applicable" to "optional". If those data fields are not reported, the report is still valuable, in our opinion.

Furthermore, we would highlight that Article 19(2) of Regulation (EU) 2022/2554 states that financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority, whereas in article 7 of the RTS it is states that *"Financial entities shall provide to competent authorities with the following information in relation to significant cyber threats with the notification in accordance with Article 19(2) of Regulation (EU) 2022/2554:"*.

Therefore, our suggestion would be to modify the wording in Article 7 of the RTS to reflect that notification for significant cyber threats is voluntary. Thus, we would propose to revise the text in Article 7 to *"Financial entities that on a voluntary basis notify significant cyber threats to the relevant competent authority, shall provide the following information in relation to significant cyber threats with the notification in accordance with Article 19(2) of Regulation (EU) 2022/2554:".*

Question 6: Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes. (**Yes**)

We noted that an incident at an ICT third-party service provider can lead to many reports when a lot of financial entities use the same ICT third-party service provider. This, combined with the fact that many questions in the intermediate and final report require input from the ICT third-party service provider leads

us to believe a more efficient way of reporting an incident should be possible where an incident affects multiple financial entities because it is caused by the same ICT third-party.

We are aligned with the single template approach to cover the initial notification, intermediate, and final reports. The report requirements seem more like a script for how the FEs are to handle their major incident processes from the ESA's perspective rather than from the individual financial entity's perspective and consequently lack proportionality.

Furthermore, as for the language requirement, it should be highlighted that English is the default language in many financial entities. Therefore, the necessity to translate into the language of the NCA could affect the speed at which they can report incidents.

Finally, as for reporting processes and channels, we would propose to have a standardised reporting template shared between ESAs and a standardized portal or process or both to submit the reports.

2 PensionsEurope answer regarding the ESA's consultation on Draft RTS on subcontracting of critical or important functions

Question 1: Are articles 1 and 2 appropriate and sufficiently clear? (**No**)

While acknowledging the related provisions in level 1, we would appreciate it if the ESAs could follow a more risk-based monitoring process in the draft RTS which will be more practical for both financial entities to implement and supervisors to enforce, based on a less rigid interpretation of the level 1. Otherwise, the draft RTS would put a disproportional burden on financial entities as they would need to diligently oversee and manage the subcontracting chain when it comes to critical or important functions. Please find our answer to answer 6 which goes further on that issue.

Furthermore, the wording in Article 1 is very unclear. Thus, it is not clear whether the elements in Article 1 must be specifically documented in the contractual arrangement (and if so, how extensive such documentation should be) or just '*taken into account*' as the current wording suggests, i.e., they are "just" general principles.

It is also not clear whether financial entities are to assess the whole chain of subcontractors based on the elements listed in Article 1(a-i). It is not acceptable to expect financial entities to evaluate the entire chain of subcontractors. It becomes evident that the administrative burden imposed on financial entities is disproportionate to the enhancement of digital operational resilience within the financial sector. In the impact assessment, ESAs indicate that '*it is therefore important to further specify a non-exhaustive list of criteria or elements of risks that can be considered by financial entities and help them in the implementation of the requirements envisaged by the RTS'*. We also believe this is very important. When reading this consideration. Article 1 should be read as a non-exhaustive list, without minimum requirements. If this is not the case, it should be indicated in the article. We suggest clarifying this.

Furthermore, more clarification is needed regarding the wording of Article 1 (f), Article 1 (g) and Article 1 (h). The current wording leaves room for different interpretations as to whether these paragraphs exclusively concern risks associated with subcontracted services (such as potential disruptions caused by subcontractors or the necessity to transition to alternate subcontractors) or, if they cover the full spectrum of risks associated with the entire ICT arrangement as a whole. We emphasize that it is disproportionate to assess risks at the subcontractor level for the whole subcontracting chain.

Furthermore, it is noted, that if financial entities are expected to individually assess transferability, disruption risk, and reintegration risk for each subcontractor, particularly in the context of standard cloud services, this requirement becomes extreme. Conducting such detailed risk assessments at the subcontractor level is not feasible for financial entities due to the complex and multi-layered nature of these services. A more practical approach would involve assessing these risks at the overall ICT service level rather than at the granular level of individual subcontractors.

Also, determining the location of data processing and storage (Article 1 (d)) might be complex in a cloud-based environment with distributed data centers. Thus, it should be clarified in what matter this should be done for cloud-based environments.

On the other hand, we agree that the parent undertaking should be responsible for providing consolidated or sub-consolidated financial statements for the group when the regulation applies on a sub-consolidated or consolidated basis.

Question 2: Is article 3 appropriate and sufficiently clear? (**No**)

Overall, we have criticism regarding Article 3. We think that the requirements listed in Article 3(1) are too extensive to be applied to all financial entities regardless of their size and risk profile and are not in line with Article 4 (proportionality principle) in the Level 1 text.

Furthermore, we find that the subcontracting risk assessments should primarily focus on major subcontractors, such as hosting service providers, rather than extending them indiscriminately to all subcontractors. Thus, many subcontractors perform relatively minor functions (for example, providing analytics or SMS services). To impose the same rigorous risk assessment criteria on these minor functions as on major subcontractors would not only be disproportionate but also impractical.

In practical terms, certain provisions such as step-in rights are not feasible in the context of cloud services. For example, neither a financial entity nor the primary ICT service provider running on a third-party cloud can realistically assume control over the operations of such hosting service provider, such as taking over a segment of Microsoft Azure's data centers to run applications independently. This highlights the necessity for making such provisions optional and applicable only in scenarios where they are realistically executable.

By differentiating subcontractors according to the significance and impact of their services, risk assessments can be customized more effectively. This approach not only aligns with the principle of proportionality but also ensures that the assessments are manageable and relevant for financial entities, especially when engaging with standard cloud services. Such a differentiated approach would facilitate a more efficient allocation of resources and attention towards those subcontractors that pose a more substantial risk to the financial entity's operations, thereby enhancing the overall effectiveness of the risk management framework.

In addition to the above, further guidance on how to comply with Article 3 is necessary. For example, at Article 3(1) c it is stated that it must be assessed "*that relevant clauses of contractual arrangements between a financial entity and an ICT third-party service provider are replicated as appropriate in the subcontracting arrangements*". It is unclear though what measures are necessary to adhere to this requirement. Should the financial entity seek copies of all subcontracting arrangements? Or is it only required that the ICT third-party service provider is contractually obligated to replicate relevant clauses in the subcontracting agreements, would this be sufficient?

Other elements, for example, Article 3(1) d, are almost impossible to document. Should the financial entity request an organization chart from an ICT third-party service provider with (possibly) an extensive number of employees in each department and team, as well as the resumés from each team's manager, etc.? Please consider whether this approach is suited to achieve the purpose.

Regarding Article 3(1) a, it is unclear if it is required that financial entities should have a mandate to set out requirements regarding operational reporting and testing directly to the subcontractor. A more appropriate approach would be to set out these requirements regarding the ICT service providers' oversight of the subcontractors in the contract between the financial entity and the service provider.

In Article 3(1) b, the phrase "when relevant and appropriate" should be clarified to define the involvement of the financial entity in the decision-making process, which should be strictly which should be strictly restricted.

Concerning Article 3(1) c, are the financial entities obligated to control agreements between ICT providers and their subcontractors? The issue is that the financial entity may not be fully aware of the contractual arrangements between the ICT third-party service provider and its subcontractor.

Article 3(1) e, is redundant as the obligations under level 1 require financial entities to have an appropriate risk management framework. Moreover, without a direct contractual arrangement between the FE and the subcontractor, the end of the sentence should be deleted: "*to monitor and oversee […] directly*". The monitoring of a subcontractor will necessarily result from clauses that will be inserted in the contract signed between the provider and the financial entity, which won't establish a direct connection between the subcontractor and the financial entity.

Finally, the article does not consider the current situation where different services are already subcontracted by ICT third-party service providers. The risk assessments performed by the financial entity at the moment of subcontracting are probably not fully compliant with the new requirements imposed by Article 3. We believe it is not realistic to have implemented this article for the current situation by January 17th, 2025, especially when ESAs are expected to deliver in July 2024, their final reports on the second batch policy product, to the Commission. We suggest a transition period for implementation concerning current subcontracted services, e.g. a year after final publication of this RTS at the OJEU.

Question 3: Is article 4 appropriate and sufficiently clear? (**No**)

This article would have an important impact on the ICT services provider's contractual liability. This could weaken the responsibilities of the provider as the financial entity would need to capture the link between the provider and the subcontractor (monitoring, audit rights, etc..).

Furthermore, the list of requirements for written contractual agreements with ICT service providers that use subcontractors is too granular. Thus, it is not realistic to expect that larger ICT service providers would agree to a contract containing all the outlined requirements. We also believe that the contractual requirements should apply only to major subcontractors, not all subcontractors.

We also want to point out that the requested specifications do not support an effective and efficient business process for subcontracting in the case of multi-client situations where multiple financial entities are outsourcing to one ICT third-party provider as is the case in the Netherlands for the pension funds industry. Especially Article 4, g) and h) provide unique, individual responses (per financial entity) which lead to customization in the contractual agreements between ICT third-party service provider and subcontractor.

Moreover, it's crucial to acknowledge the impracticality of integrating subcontractor-specific service levels and business continuity plans into contracts with the primary ICT service provider. Financial entities typically do not have access to such detailed technical information regarding every component of the service being provided. Given that the primary ICT service provider retains overall responsibility for the delivery of the ICT service, requiring financial entities to manage these specifics at the subcontractor level is not only unfeasible but also diverts attention from more critical oversight responsibilities. Instead, the focus should

be on ensuring that the primary ICT service provider upholds high-security standards of service and business continuity, which, by extension, would encompass the performance of their major subcontractor.

Furthermore, whereas it is reasonable that the financial entities shall identify which ICT service providers support critical or important functions, in many instances, it may be close to impossible to foresee which of those are eligible for subcontracting and under which conditions. This should be on a case-by-case basis, and not regulated in an RTS.

In addition, we don't find it reasonable that the financial entities are required to monitor services with the financial entities' CTTP/TPP subcontractors – and their sub-contractors (etc.) directly with the subcontractor. This should be expected to be done through the contracted CTTP/TPP otherwise we find it disproportionate.

Also, it should be clarified what is meant by "*ownership of data*" in Article 4 (d).

Furthermore, we ask for more clarification about the latter part of the sentence 'which of those are eligible for subcontracting and under which conditions'. To leave the interpretation of 'under which conditions' to the financial entity leaves room for different interpretations from written consent (which should be sufficient) to very stringent clauses (which is not desirable as this imposes even more administrative burdens on the financial entity and ICT service provider.

Finally, we would kindly ask ESAs to elaborate on whether Article 4 (f) entails that ICT third-party service providers cannot declare *force majeure* when the subcontractor cannot meet its service levels or any other contractual obligations when the ICT third-party service provider cannot substitute the sub-contractor with another sub-contractor immediately?.

Question 4: Is article 5 appropriate and sufficiently clear? (**No**)

Overall, for a financial entity, it would be very difficult to collect information on subcontractors beyond rank 2. It is rather, the ICT services provider that has a better understanding of it and could therefore give information to the financial entity. There are differences in information between the financial entity and ICT services providers as regards the ICT subcontracting chain because the financial entity has no access to certain information like the provider.

Besides the administrative burden, this article carries significant cost ramifications. Also, practical implications are not considered in this article, e.g. the fact that a financial entity does not have access to certain information as it is the indirect client and the confidentiality between a service provider and a subcontractor (and subcontractors thereof). The objective of Article 5 can also be accomplished through various interpretations, such as stringent monitoring of primary ICT service providers by the financial entities (including oversight of the ICT service provider related to outsourced services) or imposing these requirements specifically on the ICT service provider instead of the financial entity.

As for Article 5 (2), it is not realistic to expect that a large ICT service provider such as Microsoft will provide the financial entities with the contractual documentation between them and their subcontractors. Thus, the requirement should be applied directly to the ICT service providers supporting a critical or important function, making it mandatory for them to make such information publicly available, instead of making it an obligation for the end customer to request the information in question.

The requirement that financial entities should monitor the entire chain of ICT subcontractors, including monitoring key performance indicators and reviewing subcontracting documentation, is highly impractical. Such a requirement would result in an excessively heavy administrative burden and incur substantial costs for financial entities, and it also diverts attention and resources from more critical oversight responsibilities and managing actual risks. It is important to acknowledge that financial entities are already mandated to monitor their primary ICT service providers. In turn, these providers are responsible for overseeing their subcontractors and managing the related risks.

Complying with the requirement will probably prove difficult because of the confidentiality between the service provider and the sub-contractor. Perhaps the aim of Article 5 can be achieved through a review of the service providers' oversight of the sub-contractor.

Generally, the responsibilities outlined in this provision seem excessively onerous and are likely to result in considerable cost implications. It also seems like overregulation that all levels of the supply chain must be monitored with the same intensity. There should be room for adjusting control requirements based on the direct dependency on each subcontractor.

Finally, we find it inappropriate that the financial entities shall monitor subcontracting conditions, including through the review of contractual documentation between ICT third-party service providers and subcontractors. It would be more appropriate to use key performance indicators to ensure that all the conditions referred to in Article 4 are complied with along the entire ICT subcontracting chain.

Question 5: Are articles 6 and 7 appropriate and sufficiently clear? (**No**)

With the same reasoning as for our answer to question 3, we believe articles 6 and 7 do not fully support an effective and efficient business process for subcontracting in the case of multi-client situations where multiple financial entities are outsourcing to one ICT third-party service-provider as in the case in the Netherlands for the pension funds industry.

Furthermore, we find it difficult to determine the scope of Article 6 as the term “material changes” is unclear. Concerning cybersecurity, “material changes” can be understood in very broad terms.

We also find that the requirement that financial entities shall require that the ICT third-party service provider only implement material changes to subcontracting arrangements after the financial entity has either approved or not objected to the changes by the end of the notice period is not realistic to implement.

Moreover, Article 6 (3) and Article 6 (4) present a significant challenge when applied to standard multi-tenant cloud services. In such situations, it becomes unfeasible for a lone customer, even if it's a financial institution, to exert control or limit the technological progress of major cloud ICT service providers like Microsoft. The expectation that a financial entity could effectively object to or require to modify changes in subcontractors within these complex cloud environments fails to consider the practical realities of how these cloud services operate and evolve, particularly in a market dominated by major ICT players who serve a diverse and extensive customer base.

In continuation of the above, we welcome harmonisation between the RTS and the EIOPA guidelines on cloud outsourcing, in particular guideline 13 which deals with sub-outsourcing of critical and important functions.

Regarding Article 7, it's observed that the termination right comes into effect if the ICT third-party service provider makes substantial alterations to subcontracting arrangements despite objections from the financial entity or without obtaining approval within the specified notice period. The notice period can differ for different financial entities, which may complicate coordination between ICT third-party service providers and subcontractors. The financial entity won't gain any advantage from this scenario, as decisions regarding changes may be delayed or take extra time due to different notice periods. We suggest adding a more specific timeframe.

Question 6: Do you have any further comment you would like to share?

Overall, PensionsEurope thinks that the draft RTS imposes excessively burdensome regulatory requirements on financial entities, making it unrealistic to implement, especially in the context of ICT service providers offering standard cloud services not specifically tailored for the financial market.

The scope of this draft RTS seems to be too broad and would be very burdensome for financial entities for IORPs. We suggest better ensuring the application of the proportionality principle and we also question the link with the ITS regarding the register of information as this ITS only contains data regarding “material” subcontractors. The administrative burden will otherwise be disproportionate, and it is very unlikely that the financial entities will be able to obtain the required information to conduct such risk assessment and monitoring obligations on all subcontractors.

In line with the principle of proportionality, the risk assessment should consider the size of the provider to avoid a disproportionate burden on subcontractors providing a minor service.

Moreover, it's important to highlight that typical cloud services typically engage numerous subcontractors, ranging from a minimum of five to as many as fifty at the initial level alone, without even considering the entire chain. These subcontractors differ significantly in their roles and impact. For instance, some provide critical services like hosting or data connectivity, while others offer auxiliary functionalities such as user interaction analytics.

While we acknowledge the importance of maintaining a registry and imposing obligations on subcontractors that deliver a substantial portion of the contracted ICT service, it appears disproportionate to extend identical requirements for all subcontractors.

The approach could hinder financial entities from utilising most standard cloud services, including widely used solutions such as standard CRM or call center services, as all cloud service providers won’t possess the capacity (or be willing) to accommodate such stringent requirements, potentially impeding technological advancement within the finance sector.

Finally, we advocate for a regulatory approach that is more nuanced and tiered, which differentiates between subcontractors according to the significance and breadth of their services to financial entities.

3 PensionsEurope answer regarding the ESA's consultation on Draft guidelines on costs and losses from major ICT incidents

Question 1: Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest. (**No**)

Generally, we believe it's impractical to anticipate financial institutions to accurately estimate gross and net losses, particularly for smaller entities lacking experience in such tasks. Consequently, there is a risk that the figures the financial entities are committed to will be very inaccurate and thus almost not viable.
There are also many categories of costs, and the threshold of 100 000 EUR is quickly reached.

Furthermore, some of the suggested cost categories will be rather difficult to estimate with reasonable accuracy, e.g. costs for *"impaired skills of staff*" and "*costs associated with internal and external communication*". We propose that it be made clear that these costs are allowed to be rough estimates. Rigid cost calculations will also go at the expense of incident resolution in a crisis operation

It would also be helpful for the ESAs to provide strict delineations of how to determine "losses due to forgone revenues" when estimating the gross costs and losses. For example, economic projections should not have to be included.

It will be difficult for financial entities to report on the costs and losses of incidents from previous fiscal years. Cost recovery from insurance often takes months, often running across accounting years. In many cases, there will therefore be a complicated audit trail between gross and net losses to relate the compensation to the cost. Moreover, a final report one month after the incident will not have conclusive certainty on whether costs are incurred or recovered.

Finally, we would like to point out that this exercise of estimation is likely to be time-consuming and would be at the expense of resolving the incident.

Question 2: Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest. (**No**)

Regarding paragraphs 5 and 6, setting the completed accounting year as a reference period and only accounting for those costs and losses that fall within that period creates issues. Indeed, internal financial accounting processes must be modified to meet the reporting requirement as most companies have a fiscal year from January 1 to December 31. A pragmatic approach is desirable, such as referring to the general ledger.

As for paragraph 8, we would welcome ESAs to give flexibility on how the estimation is to be reflected in the annual report.

Question 3: Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest. (**No**)

PensionsEurope thinks it lacks proportionality for financial entities to be required to report both aggregated data and data for each individual major incident. There must be a balance between reporting and incident resolution to avoid extensive administrative burdens on the financial entities.

Regarding the relationship between the pension fund and its service providers, it is important that service providers can report uniformly to all their clients. Duplication of cost reporting for each financial entity should be avoided.

We would encourage the ESAs to convert the proposed template in the annex to an online platform, where the financial entities can report the estimates as well as get access to previous reports. Finally, it is not viable to determine the exact 'economic impact'. This will always be an estimate and the guidelines should reflect this.

4 *PensionsEurope answer regarding the ESA's consultation on Draft RTS on Threat led penetration tests*

Question 1: Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed. (**No**)

We would like to highlight that the systemic nature of IORPs is lower compared to other financial entities and should therefore lead to a more cautious approach for IORPs regarding TLPT processes.

The appropriateness of employing a cross-sectoral approach hinges on how the threat scenarios, which are obligatory for testing, are scoped.

For some financial entities, all the scenarios are not relevant. For example, transaction payments are mainly relevant for banks, but for pension funds, other high-risk scenarios could be useful on TLPT.

Question 2: Do you agree with this approach? If not, please provide detailed justifications and alternative wording as needed. (**No**)

Article 2 of the RTS on TLPT allows supervisors to require certain financial entities to perform TLPT, on the basis of a number of criteria. Considering that pension policy is a national competence and the IORP II Directive prescribes minimum harmonization, IORPs vary widely between Member States. That makes it hard to specify EU criteria for IOPRs on the application of TLPT. National TLPT authorities seem better placed to us to determine whether IORPs and their service providers have to perform TLPT. We think there should be stronger proportionality considerations in Article 2(3) as well as Section II of the RTS.

Article 2(3) does not appear to be proportional in the sense described in point 3.3.2. (Proportionality) of the consultation paper as it will allow for application across most participants in the financial services market instead of focusing, as announced, on "*financial entities that carry a certain degree of systemic importance and are mature enough*" (point 22). Thus, it should be clear that financial entities that pose very low risks to the continuity of core financial services such as IORPs are not within the scope of the DORA TLPT set-up. As it stands, Article 2(3) does not give financial entities enough clarity on whether they could be required to do advanced testing.

Preparation for TLPT takes considerable time. TLPT authorities should allow enough time between the assessment that a pension is required to perform TLPT and the first testing.

Question 3: Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed. (**Yes**)

While we appreciate that the proportionality principle is embedded in the two-layered approach, we are concerned that this approach could capture financial entities that do not represent major financial stability concerns such as IORPs. It must be ensured that only financial entities that play a systemic role will be part of the DORA TLPT setup.

Also, based on criteria developed by ESAs in article 2(3) of the draft RTS, national competent authorities (NCA) will assess on a case-by-case basis, which entities could be in the scope of the TLPT requirement. Thus, given their different characteristics compared to other financial entities, (not-for-profit organisation, embedded in national and social contexts) NCA should carefully assess whether IORPs should be in the scope of TLPT requirements.

Question 4: Do you agree with the proposed quantitative criteria and thresholds in Article 2(1) of the draft RTS to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed. (**No**)

Article 2 (1) refers to the by-default list of identified financial entities which rightly excludes IORPs for reasons mentioned above.

We would like to indicate that the criteria in Article 2(2) and Article 2(3) are phrased in vague terms. Thus, it will be difficult for financial entities that do not play a systemic role (e.g. the vast majority of pension funds) to determine whether they will be required to do TLPT, which is problematic as the vast majority of financial entities do not have the capabilities to perform TLPT test today, and thus need sufficient time to prepare for performing the tests (hire staff etc.).

Question 5: Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions. (**No**)

TYPE YOUR TEXT HERE

Question 6: Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT? If not, please provide detailed justifications and alternative wording as needed. (**No**)

Risk management for the TLPT is a major issue. Article 5 of the draft RTS prescribes that the control teams take measures to manage the risks and shall ensure that; 1) the threat intelligence provider provides at least three references from previous assignments related to intelligence-led red team tests (as provided by paragraph 2, subparagraph c); 2) the external testers provide at least five references from previous assignments related to intelligence-led red team tests (as provided by paragraph 2, subparagraph d).

It is likely to be problematic. Companies that are subject to TLPT, or comparable testing often do not wish to be named as a company that is subject to testing, given the reputational risks associated.

Question 7: Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed. (**No**)

We would like to highlight that the draft RTS is going beyond the level 1 empowerment which does not give a mandate to ESAs as regards criteria for external testers.

To introduce additional requirements is not only legally problematic. It will also lead to increased costs and administration burdens for the financial entities.

Question 8: Do you think that the specified number of years of experience for external testers and threat intelligence providers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills? If not, please provide detailed justifications and alternative wording as needed. (**No**)

We believe that the number of years of experience for testers lacks rationale and is not flexible enough. A staff member of the threat intelligence provider might have 4.5 years of experience instead of 5 years, and therefore not qualify according to the draft RTS. It might also be counterproductive and limit the number of threat intelligence providers or external testers while not necessarily improving the quality of said parties.

Overall, the requirement will harm the number of potential providers of TLPTs and the effect on the financial entities' opportunity to comply with the RTS.

As an alternative, we suggest sticking to a more principle-based requirement and requiring instead 'a proven track record' for external testers and threat intelligence providers.

Question 9: Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed. (**No**)

Article 4(2), subparagraph c of the draft RTS states that the control team is informed of any detection of the TLPT by staff members of the financial entity or of its third-party service providers, where relevant, and the control team encompasses the escalation of the resulting incident response, where needed.

This seems to be counterproductive and not aligned with the purpose of a TLPT. Besides the TLPT team carrying out the exercise, nobody within the company (i.e. the tested entity) knows about an ongoing TLPT. The control team cannot be informed if staff members have detected a TLPT. That would imply that every suspicious activity needs to be communicated to the TLPT team, even when that is not part of a TLPT. This would result in an extra reporting activity, and it would also imply that people within the organization know who is part of the control team (i.e. which is not always in function).

We note that testing is only feasible with direct contracting parties. Financial entities should not be required to test further down the subcontracting chain. The RTS could clarify this.

Question 10: Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed. (**No**)

It should be specified that a pooled testing exercise is possible between different financial entities within the same group when it comes to shared critical business functions provided by an internal shared IT service provider. In other words, it should be allowed to have one pooled testing performed and shared among financial entities of the same group using the same intra-group provider.

Question 11: Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed. (**No**)

It is important to emphasize that Level 1 does not authorize ESAs to specify the criteria for external testers. The criteria set at level 1 are sufficient and more appropriate, as they notably require using testers that are certified or adhere to a code of conduct or an ethical framework (Article 27, 1. (d))

Criteria for the in-house testers seem to be difficult to implement due to their granularity and do not give enough flexibility to financial entities such as IORPs.

The criteria for in-house testers are too restrictive and will make it difficult to use in-house testers. As the market for external testers is very tight, this is likely to constitute a major practical obstacle to the implementation of TLPTs.

At the very least, the requirement to have been with the company for two years should be limited to a single member of the testing team (Article 11 (1) (a) (ii)) of the draft RTS.

Question 12: Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed. (**Yes**)

TYPE YOUR TEXT HERE

Question 13: Do you have any other comment or suggestion to make in relation to the proposed draft RTS? If so, please provide detailed justifications and alternative wording as needed.

First, it is difficult to see how proportionality is considered regarding the types of financial entities that do not fall under Article 2(1) and the requirements outlined in the relevant articles in section two of the RTS.

Second, we find it inappropriate that the TLPT Authorities are tasked “to organise” and “to lead” the tests as we do not find that a TLPT test is an oversight activity. The authorities should review the results of the tests, but they cannot both lead a test and evaluate the results of the test impartially. In addition, the approach is not aligned with Article 26 and Article 27 of the Level 1 text.

We also notice that the draft RTS does not include the obligation for the TLPT authority to set up ‘Chinese Walls’ (i.e. barriers to information) between the internal TLPT team of the TLPT authority and its regular supervisory teams (e.g. prudential and conduct of business supervision). The outcomes of the TLPT authority should not result in enforcement by the ‘regular’ supervisory team of the TLPT authority or other NCAs. We suggest adding the requirement of Chinese walls within the TLPT authority to either Article 2 or 3 of the draft RTS.

The TIBER-NL framework prescribes that the testing authority gets informed about the preparation and performance of TIBER testing. The authority can only access the documentation at the financial entity’s premises, to prevent this very sensitive information is concentrated at one point. The DORA RTS mandates to provide the TPLT authority with this information. There are doubts about the wisdom of this decision.

5 *PensionsEurope answer regarding the ESA's consultation on Draft RTS on oversight harmonisation*

Question 1: Do you agree with the content of information to be provided by ICT third party providers in the application for a voluntary request to be designated as critical? Please, provide comments on information to be added or removed including the rationale (Article 1) (**No**)

We are concerned about the administrative burden generated to comply with all the requirements, especially for small and medium-sized financial entities connected with the critical ICT third-party provider. This applies to the information demanded in Articles 1, 3, 6, and 7.

In continuation hereof, we would propose that the content of the information that is to be provided by the ICT third-party provider should be completely aligned with the financial entities' *register of information* so that financial entities are not required to request additional information.

Setting up and maintaining the *register of information* will be an extremely time-consuming exercise. Therefore, the administrative burden on financial entities should be reduced as much as possible. One way to ensure this is that the ESAs share the information they have received from the CTPPs with the financial entities. In this way, the financial entities shall only collect information concerning "regular" ICT third-party providers and not the CTPPs.

Question 2: Is the process to assess the completeness of opt-in application clear and understandable? (Article 2) (**No**)

We wonder why an ICT third-party provider would voluntarily request to be designated as a CTPP in light of the heavy regulatory burden that will be the result of the designation.

It is unclear what would be the outcome of the process if a third-party provider is designated as a critical third-party provider. Is this to be made public on a whitelist?

Question 3: Is the list of information to be provided by critical ICT third-party service providers to the Lead Overseer that is necessary to carry out its duties clear and complete? Please, provide comments on information to be added or removed including the rationale (Article 3) (**Yes**)

TYPE YOUR TEXT HERE

Question 4: Do you agree with the content of Article 4 on remediation plan and progress reports?

TYPE YOUR TEXT HERE

Question 5: Is the article on the structure and format of information provided by the critical ICT third-party service provider appropriate and structured? (Article 5) (**Yes**)

TYPE YOUR TEXT HERE

Question 6: Is the information to be provided by the critical ICT third-party service provider to the Lead Overseer complete, appropriate and structured? (Article 6 and Annex I) (**Yes**)

TYPE YOUR TEXT HERE

Question 7: Is Article 7 on competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer clear? (**No**)

According to Article 7 (2) a, the CAs must take into consideration "*the remediation measures implemented by financial entities to mitigate risks*" connected to using a CTTP. However, the method through which financial entities should communicate information to the CAs remains unclear. Additionally, the anticipated administrative costs for financial entities to meet this requirement are not yet specified. A thorough impact assessment would be appreciated.

Furthermore, according to Article 7 (4), "*CAs shall request to financial entities any information necessary to carry out the assessment specified in paragraph 1*" of the Article. We find it inappropriate to impose an administrative burden on a financial entity about oversight activities that do not have the financial entity as the subject.

Question 8: Do you agree with the impact assessment and the main conclusions stemming from it? (**Yes**)

We agree with the ESA's assessment that the draft RTS will lead to additional compliance efforts for the financial entities as they must invest in new systems and processes to ensure compliance with the requirements in the RTS. Moreover, implementing RTS will impose additional administrative burdens on financial entities.

However, the impact assessment is not transparent though concerning the extent of the administrative burdens. For instance, it is not clear what the remediation measures implemented by the financial entities entail.

6 *PensionsEurope answer regarding the ESA's consultation on Draft guidelines on oversight cooperation between ESAs and competent authorities*

Question 1: For each guideline, do you consider the Guideline to be clear, concise and comprehensible? If your answer is no, please refer to the specific point(s) of the guideline which is/are not sufficiently clear, concise or comprehensible. (**No**)

It would be appreciated if guideline 13 could include an in-depth description of the measures that the competent authorities (CAs) can impose on the financial entity (FE) under Article 42 (Follow-up by competent authorities) and Article 50 (Administrative penalties and remedial measures) in the Level 1 text as well as provide scenarios for the measures. The current wording is ambiguous and thus makes it difficult for the FEs to navigate with the use of critical third-party providers (CTPPs) as third-party providers.

Furthermore, we would invite ESAs to clarify the term *"other additional information as deemed useful"* in guideline 9 as it lacks precision and may leave considerable room for interpretation.

Question 2: Taking into account the specific scope of these Guidelines, do you consider that these Guidelines cover all the instances where cooperation and information exchange between CAs and the LO is necessary? If your answer is no, please propose additional areas that should be covered.

TYPE YOUR TEXT HERE

Question 3: Do you consider that the implementation of these Guidelines will contribute to adequate cooperation and information exchange between the ESAs and CAs in the conduct of oversight activities? If your answer is no, please propose an alternative approach how this could be achieved. (**Yes**)

However, the guidelines are only concerned with the information to be provided by the CAs to the lead overseer (LO). It is equally important to ensure that the financial entities are constantly informed about findings and conclusions.

In this way, the financial entities will be able to consider such information as part of upcoming outsourcing arrangements and processes, ensuring ongoing compliance. In continuation hereof, it is important to keep in mind that one of the purposes of Article 30 in the level 1 text is to balance the negotiation power between the financial entities and the third-party providers.

Question 4: What are your main expectations regarding the impact on financial entities and CTPPs of the application of these Guidelines?

Overall, it is hard to say how these guidelines will impact FEs and CTPPs. Thus, it would be helpful if the ESAs could provide a more comprehensive description of the lead overseer mandate to dictate or enforce a financial entity to depart a contract with a CTPP if the withdrawal could affect financial stability.

Also, have the ESAs considered a scenario where some TPPs or CTPPs do not wish to provide their service to FEs in the EU due to the extensive requirements?

About PensionsEurope

PensionsEurope represents national associations of pension funds and similar institutions for workplace and other funded pensions. Some members operate purely individual pension schemes. PensionsEurope has **25 member associations** in 18 EU Member States and 3 other European countries[1].

PensionsEurope member organisations cover different types of workplace pensions. In addition, many members of PensionsEurope also cover personal pensions, which are connected with an employment relation.

PensionsEurope also has **18 Corporate and Supporter Members** which are various service providers and stakeholders that work with IORPs.

PensionsEurope has established a **Central & Eastern European Countries Forum (CEEC Forum)** to discuss issues common to pension systems in that region.

PensionsEurope has established a **Multinational Advisory Group (MAG)** which delivers advice on pension issues to PensionsEurope. It provides a collective voice and information sharing for the expertise and opinions of multinationals.

What PensionsEurope stands for

- A regulatory environment encouraging workplace pension membership;
- Ensure that more and more Europeans can benefit from an adequate income in retirement;
- Policies which will enable sufficient contributions and good returns.

Our members offer

- Economies of scale in governance, administration and asset management;
- Risk pooling and often intergenerational risk-sharing;
- Often "not-for-profit" and some/all of the costs are borne by the employer;
- Members of workplace pension schemes often benefit from a contribution paid by the employer;
- Wide-scale coverage due to mandatory participation, sector-wide participation based on collective agreements and soft-compulsion elements such as auto-enrolment;
- Good governance and alignment of interest due to participation of the main stakeholders.

Contact:
PensionsEurope
Montoyerstraat 23 rue Montoyer – 1000 Brussels
Belgium
Tel: +32 (0)2 289 14 14
info@pensionseurope.eu

[1] EU Member States: Austria, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, Netherlands, Portugal, Romania, Spain, Sweden. Non-EU Member States: Iceland, Norway, Switzerland, UK.