PensionsEurope answer regarding the ESA's consultation on Draft RTS on classification of ICT incidents

Joint European Supervisory Authority Consultation paper on DORA

September 2023

www.pensionseurope.eu

Question 1: Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest. **(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.

However, we want to highlight that the characteristics, specificities, and operations of institutions for occupational retirement provision (IORPs) and their service providers have not been properly considered in the ESAs preliminary approach. This is recognised in the level 1 regulation at Recital 21, referring to the proportionate approach that competent authorities must maintain regarding IORPs, "which (…) outsource a significant part of their core business, such as asset management, actuarial calculations, accounting, and data management, to service providers". The EU pension landscape is very fragmented with many pension funds having few beneficiaries. The above-mentioned features mean that most of the ICT incidents would trigger the relative criteria of affected financial counterparts and the qualitative criteria for critical services affected.

We encourage ESAs to reconsider entity-specific deviations for IORPs from the criteria and thresholds indicated in this consultation paper to ensure a proper application of the framework by IORPs which are distinct from other financially regulated entities. Indeed, IORPs are institutions strongly embedded within national social models.

Furthermore, we are of the opinion that the methodology established by ESAs is not sufficiently considering the materiality dimension of ICT-related incidents. It would be counterproductive for the supervisor to scrutinise ICT incidents that are not deemed to be material because of criteria that the ESAs put forward. Moreover, it would unnecessarily increase the burden on both supervisors and IORPs. We therefore believe that the *clients, financial counterparts, and transactions affected* criteria should not be primary criteria as it doesn't ensure a proportionate treatment for IORPs.

We would invite the ESAs to put the materiality principle as a prerequisite to consider an ICT-related incident as a major incident to ensure that it affects a service that supports a critical or important function. Therefore, within the different primary criteria, we consider that *critical services* and *data losses* should be essential criteria to define an incident as major.

Finally, we are satisfied that the reputational impact criteria is being considered as secondary criteria. There is no metric to assess reputational damages like the time after which the damage would be undone. If an ICT- related incident is covered by the media, it can give a biased view of the impact on the organization and its customers.

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? If not, please provide your reasoning and suggested changes. **(No)**

The model proposed in Articles 1 and 9 of the draft RTS is likely to lead to overreporting without any concrete benefit regarding strengthening digital operational resilience.

Indeed, the design itself of the criterion "*clients, financial counterparts, and transactions affected"* can be questioned as any of the conditions being fulfilled can trigger this criterion. We do not think that is a

proportionate approach for the pension funds sector and we would suggest instead, implementing a two-condition cumulative approach. Reaching at least two conditions of this criterion would trigger it and would also lead to a better allocation of resources for national competent authorities when enforcing the new digital operational framework.

PensionsEurope is also concerned that with the proposed specifications and thresholds, most ICT-related incidents will be classified as major because pension funds service providers have only a few financial counterparts. Furthermore, as ICT tools provided by service providers are being mutualized and are identical for each client, there is a huge risk that most ICT-related incidents would trigger the 10% relative threshold for the *number of financial counterparts affected.* To ensure a proportionate treatment of IORPs, we would propose a cumulative floor to trigger this condition if at least 20 financial counterparts are affected

Finally, regarding the "relevance of the clients or financial counterparts' part of the criterion (Article 1, paragraph 3), we believe that the specificities of pension funds should be considered as recognized by Recital 21 of DORA. Thus, this part of the criterion "*clients, financial counterparts, and transactions affected*" *should* not apply to the pension fund's service provider as any incident would affect the implementation of the business objectives of the pension fund. Indeed, pension funds have often small structures that offer only pension schemes to members and beneficiaries thanks to the support of service providers. Those latter provide regular service to a restrained number of pension funds.

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 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? If not, please provide your reasoning and suggested changes. **(No)**

For the duration and service downtime threshold, PensionsEurope would like to draw attention to the inappropriateness of the 2-hour service downtime for the pensions funds sector as it seems to be inspired by the banking and payment services. Indeed, IORPs would be affected by such thresholds as financial entities with no incident reporting requirements prior to DORA. Furthermore, IORPs' activities are usually split between asset management and pension administration services.

For asset management services, essential functions regarding duration and service downtime are limited to trade repositories and the administration of other financial transactions such as integrated investment management systems, and the hosting of these systems. Without these systems, it is not possible to perform trades. Their downtime creates issues with fulfilling contractual and legal obligations. Regarding trade repositories, as the ESAs are willing to replicate existing service downtime requirements on those for all financial entities, the 2-hour service downtime threshold for ICT-related incident reporting is already in place and should be applicable for other trade administration systems.

For pension administration services, the interval of the use of services is a key parameter and we consider collecting pension contributions, payment of pension benefits as well as the updates of pension entitlements as supporting critical functions. The three above-mentioned tasks are made or updated monthly. Therefore, pension administration services are used only for a limited number of hours during one day of the month. Those hours in the system should be seen as service downtime for paying pension benefits, collecting pension contributions, and updating pension entitlements. We are of the opinion that the service duration threshold of two hours is reasonable for the use of services during these hours. On the other hand, outside of the hours when services are working, incident duration should not be seen as service downtime.

Nevertheless, it remains essential to ensure the availability and integrity of pension data outside of the hours when pension administration services are working. Any ICT-related incident affecting those services would negatively impact pension funds' members and participants in the medium and longer term. We considered that those issues are better tackled within the criterion of *data losses* instead of the *duration and service downtime* criterion.

We also want to point out that in Article 3, paragraph 1, the word "resolved" lacks details and would need to be defined to let the financial entity have a proper view of the duration of the ICT incident and its resolution. For consistency reasons, we suggest applying the same "end" criterion as for the termination of service downtime with "the moment when regular activities and operations have been restored to the level of service that was provided prior to the incident".

Regarding the reputational impact, as indicated in our answer to question 1, we believe that if an incident is being covered by the media, that does not necessarily give a factual view of the impact on the organization and its customers. Therefore, this criterion is hard to enforce for supervisors and would be hard to use in the classification of ICT-related incidents with the proposed specifications. Therefore, instead of those specifications, it seems appropriate to assess the reputational impact in terms of its impact on complaints, meeting regulatory requirements, and/or losing clients or financial counterparts.

Finally, for the economic impact criteria, we would prefer to increase the threshold for material damage from 100 000 euros to 1 million euros as the proposed threshold would not apply mainly to large financial entities as assumed by the ESAs. Furthermore, it is difficult to assess the gross direct and indirect costs and losses incurred by the incident, especially the staff costs. Therefore, raising the threshold would ensure a better proportionate approach for IORPs.

Question 4: Do you agree with the specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13? If not, please provide your reasoning and suggested changes. **(No)**

"Data losses" would need to be defined before setting the specification and threshold of the criterion "data losses". PensionsEurope also thinks that guidance is needed on the relationship between Articles 33 et 34 of the GDPR and DORA's "data losses" criterion, especially on measures to avoid reporting delays.

Question 5: Do you agree with the specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14? If not, please provide your reasoning and suggested changes. **(No)**

PensionsEurope believes that the *critical services affected* criterion as proposed would not capture specific cases but rather a wide range of incidents, leading to overreporting. Indeed, the related threshold asks financial entities to report if any critical service has been affected and whether the incident has escalated to its senior management or management body. Those specifications are too broad and not proportionate by nature.

As many services require authorization, it seems also that the specification of the provision of financial services that require authorization and registration in the EU touches upon the authenticity, integrity, and, or confidentiality of data, which is already covered in the criterion 'data losses'. It would be redundant with the latter primary criteria, thereby triggering two primary criteria at once. A qualitative 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? If not, please provide your reasoning and suggested changes. Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents). **(Yes)**

PensionsEurope agrees mostly with the overall approach taken. Improvements can be made as financial entities would need a standardised way in Information Technology Infrastructure Library (ITIL) to do so and precisions would need to be provided to define "recurring" to avoid capturing even minor incidents.

Question 7: Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes. **(No)**

While we appreciate the ESAs approach to incorporate materiality thresholds for determining significant cyber threats, we believe that the phrasing in Article 17 leaves too much room for interpretation as there is no clear definition of "high probability of materialisation" in paragraph 1 (b) for this condition determining a cyber threat.

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? If not, please provide your reasoning and suggested changes. **(No)**

The ESA's approach regarding whether major ICT-related incidents are relevant for competent authorities in other Member States starts with good intentions. However, we are uncertain about the consequences if a major incident impacts a non-Member States and the possibility of harmonising existing rules as existing national rules imply that incidents affecting clients in several Member States need to be reported to all NCAs.

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 4 other European countries[1].

PensionsEurope member organisations cover different types of workplace pensions for over **110 million people.** Through its Member Associations PensionsEurope represents **€ 7 trillion of assets** managed for future pension payments. In addition, many members of PensionsEurope also cover personal pensions, which are connected with an employment relation.

PensionsEurope also has **20 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.

PensionsEurope answer regarding the ESA's consultation on Draft RTSs ICT risk management tools methods processes and policies

Joint European Supervisory Authority Consultation paper on DORA

September 2023

www.pensionseurope.eu

Question 1: 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.

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.

To ensure a well-functioning framework, we believe there is a need to further include the proportionality principle within Title 1 as we are of the opinion that the underlying requirements are very granular and not tailored for occupational pensions which follow a monthly cycle of operation. IORPs are distinct from other financial entities with their specificities as they are embedded in national social and labour law. The level of detail in the draft RTS is so high that makes the application of Article 4 of the DORA regulation related to the proportionality principle difficult for national competent authorities.

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. 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 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.

Therefore, we are of the opinion that the principle of proportionality which is well-anchored in DORA should be better reflected in the draft RTS. DORA should allow a risk-based and principle-based approach to DORA requirements. 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.

We propose to modify Article 29 of the RTS to explicitly refer to the application of the principle of proportionality, as follow:

"For the purposes of defining and implementing ICT risk management tools, methods, processes, and policies referred to in Articles 1 to 28 elements, financial entities shall implement the rules in accordance with the principle of proportionality, considering their size and overall risk profile, and the nature, scale, and complexity of their services, activities, and operations. "

This will ensure that the principle of proportionality is correctly applied by national competent authorities and will allow financial entities to lower implementation costs according to their structures and address the increasing complexity resulting from the implementation of the RTS, as proposed. A fundamental 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.

Question 2: 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.

Title II of the proposed draft RTS refers to Article 16 of DORA which established a lighter ICT regime for pension funds for small institutions for occupational retirement provision which does not have more than 100 members in total. While we fully understand that this threshold is a level 1 issue, we think putting IORPs with more than 100 members in the same category as systemic banks or insurers for instance would not consider the specificities of IORPs. The activities of a pension fund cannot be compared to the operations of banks and insurers. Pension funds make payments once a month, compared to the high number of financial transactions proceeded by banks.

Question 3: Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

We are satisfied with the approach concerning the provisions on governance if only a general, overarching rule of proportionality is included, as proposed, in our answer to question 1.

Furthermore, we suggest amending Recital 3 of the draft RTS as follows to ensure a different reading of the related article 1 and 2 of the draft RTS:

Considering leading practices and, where applicable, relevant international standards, financial entities should develop and implement consistent and up-to-date ICT security policies that support the financial entity's digital operational resilience strategy and the related information security objectives. To ensure compliance, enhance the overall information security awareness and culture of the financial entity, and prevent unintentional security breaches, the ICT security policies should be approved by the management body of the financial entity. Where the financial entity deems it necessary, the security guideline may also be made available to third parties (e.g. stakeholders or service providers).

Question 4: Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.

Article 3 of the draft RTS will make its enforcement difficult for national competent authorities because of its different structure compared to level one, despite both level one and the RTS using the same terminology. Considering the multitude of different types of documented actions required by levels 1 and 2 is also causing confusion. Those two reasons are making it difficult to assess which precise requirements of the DORA regulation are addressed in Article 3 of the draft RTS.

Question 5: Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.

PensionsEurope believes that the level of detail in Articles 4 and 5 of the draft RTS is too high compared to the level one regulation. Article 3(7) of the DORA regulation defines ICT assets very broadly as "a software or hardware asset in the network and information systems used by the financial entity" and Article 8(4) of the DORA regulation requires to identify of each asset and to map those deemed critical. Furthermore,

Article 8(6) of the DORA regulation requires also that financial entities shall maintain relevant inventories and update them periodically.

We believe that giving unique identifiers to each asset as provided by the draft RTS, regardless of its criticality, would already constitute an act of "mapping", especially since the draft text expects the financial entity to document additional information on the location, either physical or logical, of all ICT assets. The volume of data required is very high without concrete benefits.

We, therefore, suggest that in Article 4(1) of the draft RTS, it should be stated that only relevant ICT must be considered in this context to exclude minor items such as screens, keyboards, or mouses for instance.

Moreover, we also propose the following change to Article 4(2) of the draft RTS: "2. The policy on the management of ICT assets may for example: (….)". This would avoid the predictiveness of the suggested approach and would avoid seeing all the ICT assets being captured.

Question 6: 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?

For operational reasons, it would be difficult to keep for all systems a record of the end date of the support. To make it work in practice, we would propose to establish a requirement to record all updates and patches and to select all ICT assets that have not been updated for 12 months.

Question 7: Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

Article 6(4) of the draft RTS related to policy on encryption and cryptography goes beyond the level 1 regulation in Article 9(4) (d) which does not require a formal policy. The prescriptive approach taken by the ESAs should be rather shifted into a more principle-based approach by ensuring the encryption of data during storage and transmission in accordance with protection requirements according to the nature of the data in question. Thus, for publicly available data and data that are classified as low risk, it should be possible to make the decision not to encrypt it, which would need the draft RTS to be changed which does not allow this choice. The same reasoning applies to data that scores low on the CIA triad (confidentiality, integrity, and availability) which is a model for the development of security systems.

Question 8: 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.

For operational reasons, as IORPs are often entities with few human resources, we do not think that any further requirement such as new measures or control to be helpful.

Question 9: Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

We are not aligned with the suggested approach to ICT operations security. The prescriptiveness of the approach would harm smaller or medium-sized IORPs which would struggle to fulfil these requirements.

For instance, the requirement in Article 10, paragraph 2 (c) which aims to "ensure that ICT third-party service providers handle any vulnerabilities to the ICT services provided to the financial entity" would need to be proportionate and more risk-based as it would lead to overreporting as every vulnerability would need to be communicated by all parties in the ICT chain.

Furthermore, Article 9, paragraph 1 would also oblige financial entities to identify the capacity requirements of their ICT systems and implement monitoring procedures as well as resource optimisation. As pension funds follow a steady rate of operations for pension administration notably, it leads to a high degree of predictability plannability which would lead the proposed required under paragraph 1 to be disproportionate.

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 and 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) also creates very granular security rules for the use of private non-portable endpoint devices as for portable endpoint devices. We think it is not a realistic risk that a financial entity's data would be wiped from a distance. This rule would effectively make the use of (private) endpoint devices such as laptops and phones impossible.

Finally, Article 12, paragraph 2(c) requires the logging of events related to change management, access control, capacity management, and network traffic activities to enhance monitoring capabilities. The volume of information to be logged is too high and it is likely to produce a lot of false positives. Researching them would also be time-consuming, which then cannot be deployed on other essential issues.

Question 10: 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.

As the level of granularity of the draft RTS is already very high and puts a disproportionate burden on financial entities, we do not believe that further measures should be taken into consideration.

Question 11: 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.

If retained, this approach would unnecessarily overburden many of the organisations within the pension funds sector. A more risk-based approach would be preferable with gradations in the scope of ICT assets, targeting assets supporting critical and important functions.

Question 12: 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.

PensionsEurope agrees with the requirements for cloud computing resources which are sufficient and does not foresee additional measures.

Question 13: Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.

PensionsEurope fully understands the importance of network security measures to ensure digital operational resilience. However, it would be appropriate to better tailor such measures to the complexity of the financial entities which is not guaranteed with Articles 13 and 14 which introduce very prescriptive measures such as mapping and visualisation of networks. Paragraph 1(c) of Article 13 requires the segmentation of the ICT administration network, leading to major changes to the network infrastructure for many financial entities. Thus, the extremely detailed requirements are likely to overwhelm numerous small and medium-sized financial entities such as IORPs.

Question 14: 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.

TYPE YOUR TEXT HERE

Question 15: Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

We do not see the added value of Article 16 draft RTS on systems acquisition, development, and maintenance which can be considered as an IT project under Article 15 of draft RTS. Furthermore, requirements introduced by Article 16 are overly prescriptive and would harm small financial entities like IORPs.

Article 16, paragraph 4 also introduces a requirement to do a source code review. We believe that 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 therefore believe that pension funds should be able to count on cybersecurity product quality assurances, which is in line with EU digital contract rules.

Furthermore, the requirement to report to the management board in Article 15 (5) of the draft RTS is unclear with the use of words or sentences "impacting", "periodically" and "depending on the size of the ICT projects" which are vague.

Question 16: Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.

We do not think that specific elements regarding the supply chain should be taken into consideration in the RTS as the Commission is not empowered to deliver such elements in the level 1 regulation.

Question 17: Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.

TYPE YOUR TEXT HERE

Question 18: Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

PensionsEurope believes that the suggested approach is not tailored for smaller organisations.

Question 19: 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.

TYPE YOUR TEXT HERE

Question 20: Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

The level 1 regulation in Article 13 (6) foresees training and awareness for all staff members without requiring specific frequency and by taking their functions into account. Therefore, Article 19 of the draft RTS is going beyond level 1 by requiring programs and training for staff conducted at least yearly without specific consideration to their positions. Therefore, it appears to be too perspective and we propose alternative drafting in Article 19 (2) to introduce lighter requirements with " The programmes and training shall be conducted continuously and with appropriate awareness and financial entities shall implement processes to regularly evaluate and review their effectiveness and to incorporate lessons learned from their analysis of the ICT-related incidents and cyber threat information into their ICT security awareness programmes and digital operational trainings.

Question 21: Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.

Requirements on human resources policy for third-party service providers should be standard. However, we are concerned that level 2 is going beyond level 1 regarding the section on Human Resources.

Article 15 (b) of DORA mandates the ESAs to "develop further the components of the controls of access management rights referred to in Article 9(4), point (c) and associated human resource policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risk through appropriate indicators".

However, Article 20 (1) b i. in the draft RTS implies requirements for staff and ICT third-party service providers to "be informed about and adhere to, the financial entity's ICT security policies, procedures and protocols", thus exceeding the scope of Level 1.

Question 22: 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.

As we believe that the draft RTS is sufficiently extensive and granular, we do not see any new measure or control that should be taken into consideration in the text.

Question 23: 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.

TYPE YOUR TEXT HERE

Question 24: Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

As the pensions fund usually follows a monthly cycle for its operations, the approach proposed on ICT business continuity management is not tailored for IORPs but rather for payment or the banking sectors. Therefore, distinctive characteristics of IORPs should be reflected in business continuity management, otherwise, overly detailed specifications can be counterproductive.

Furthermore, Article 27, paragraph 2 prescribes a very extensive amount and specificities of scenarios to identify that the measure is losing its focus. Only scenarios that are relevant to the financial entity should be examined. Scenarios that do not or cannot apply to the institution at all or whose probability is extremely low will only lead to disproportionate burdens and high costs.

Question 25: Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

TYPE YOUR TEXT HERE

Question 26: 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.

PensionsEurope welcomes that proportionality criteria are to be embedded in the reports on the ICT risk management framework. However, this cannot counterbalance the insufficient integration of proportionality in the remaining text of the draft RTS with such an extensive report. Furthermore, with the proposed technical content as planned in a very prescriptive Article 28, the report is not appropriate for the entire management but rather for specific IT managers. Currently used formats that provide an overview for board members of most of the pension funds would not be allowed under the proposed report.

Question 27: Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.

As proposed, the simplified ICT risk management framework is not really "simplified" as it cannot allow IORPs affected to implement a flexible approach related to their digital operational resilience plan. This simplified framework is still granular which makes the differentiation between the simplified and the standard framework difficult.

Question 28: 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.

TYPE YOUR TEXT HERE

Question 29: 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.

We believe expanding the ICT operation security for all ICT assets would imply additional running and building costs, which can be disproportionate for small entities in opposition to the aim of DORA.

Question 30: 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.

TYPE YOUR TEXT HERE

Question 31: 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.

TYPE YOUR TEXT HERE

Question 32: 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.

TYPE YOUR TEXT HERE

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 4 other European countries[1].

PensionsEurope member organisations cover different types of workplace pensions for over **110 million people.** Through its Member Associations PensionsEurope represents **€ 7 trillion of assets** managed for future pension payments. In addition, many members of PensionsEurope also cover personal pensions, which are connected with an employment relation.

PensionsEurope also has **20 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;

[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.

- 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

PensionsEurope answer regarding the ESA's consultation on Draft RTS on policy on the use of ICT services regarding CI functions

Joint European Supervisory Authority Consultation paper on DORA

September 2023

www.pensionseurope.eu

Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear? **(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. The level 1 regulation already provides for proportionality for the supervision of IORPs which are outsourcing "a significant part of their core business" as recognised in Recital 21.

However, we are concerned that the proportionality principle as prescribed by Article 4 of the level 1 regulation is not sufficiently considered in Article 1 of the draft RTS as it will oblige affected IORPs to ensure transparency throughout the whole outsourcing chain but also beyond the outsourcing process. The lighter regime for IORPs with fewer than 100 participants as foreseen by the level 1 regulation does not sufficiently address our concerns as it doesn't capture the majority of the IORP's pension landscape. We, therefore, think that the policy on the use of ICT services regarding critical and important functions should be designed in consideration of the principle of proportionality. This can be done by explicitly referring to Article 4 of DORA in Article 1 of the draft RTS.

While we do not oppose the ESAs willingness to increase transparency on outsourcing operations, we are of the opinion that this increase in transparency must be cautiously balanced with the operating model of IORPs which need the flexibility to function properly.

PensionsEurope appreciate the choice made by European Supervisory Authorities to refer to the definition of 'critical or important functions' stipulated by DORA, rather than providing more detailed criteria in the RTS. This makes it possible to tailor approaches to different sub-sectors in the financial sector.

We would also like to get more clarity on "the nature of data shared with the ICT third-party service providers" as defined by the draft RTS in Article 1 as data can be assessed from multiple points of view either on the side availability, integrity, or confidentiality, which could not be aligned with the aim of DORA.

PensionsEurope also has a remark regarding the lack of clarity in Article 1 which has one long sentence. The terminology being used is also unclear as it uses the terms "increased complexity or risk" which does not refer to proper criteria to determine such an increase.

Regarding Article 2, as the Pension sector mostly has organisations operating within one member state with a centralised organisational structure such as in the Netherlands, it is not impacting our sector. We therefore believe Article 2 is clear and appropriate.

Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear? **(No)**

There are already existing governance requirements in place within most of the organisation in the pension funds sector, despite not being documented in one specific policy on the use of ICT services supporting critical or important functions. The added value of having this documented in one policy is questionable and must be left to the discretion of the NCA.

As regards paragraph 2, doing a "regular" with a frequency of at least once every three years instead of a yearly review should be enough to avoid disproportionate costs and ensure a risk-based review.

Furthermore, to provide more clarity, paragraph 6 could be slightly reviewed by replacing "monitoring the relevant contractual arrangements" with "overseeing and strategically monitoring the contractual arrangements".

Finally, paragraph 8 requires an independent review of ICT services supporting critical or important functions provided by ICT third-party service providers. If pension funds are already using independent sources to undertake such reviews, it is not possible to generalise this requirement to all assessments due to the lack of publicly available independent assessments. Thus, we propose to make this independent review on a voluntary basis in addition to granting financial entities the possibility to perform an internal audit. The latter approach should consider the relationship between pension funds and services providers as recognised by Recital 21 of DORA with pension service providers performing a review of ICT third-party service providers.

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

PensionsEurope thinks that Article 4 is not clear and lacks precisions. Its aim, wording, and structure are vague.

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

Article 5 is clear but not appropriate as pension funds are outsourcing most of their core activities as recognized by Recital 21 of DORA. Requirements related to managing contracts and third parties during the duration of the contract, as well as having a 'Know your customer' process in place are often already in place within the pension funds sector. However, those requirements would be ineffective as pension funds often outsource the management of third-party providers to their main processor or ICT services provider. To reflect on the specificities of pension funds as recognized by Recital 21, It would be helpful if contract and third-party management could be delegated to the main ICT services provider, which will otherwise be the impacted entity of the process.

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

Article 6 is clear and relatively appropriate as risk assessment is being undertaken by most of the pension funds. However, we want to highlight that the approach proposed by the ESAs would make sense at the financial entity level only for concentration risk as planned by Article 29 of DORA. Thus, many risks need to be assessed locally.

Regarding Article 7, provisions are relatively clear and partially appropriate. Implementing a due diligence assessment prior to contracting a third party is not a new practice within the pension funds industry. However, Article 7 (1a) is not sufficiently clear when requiring financial entities to assess whether the ICT service provider has "the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate" as we are not certain how those entities would actually assess this.

We also approve the development of ethical and socially responsible business practices. However, we do not think that DORA is the right framework to introduce such a due diligence check as DORA should focus on mitigating ICT risk in the financial sector. It would therefore be appropriate to remove Article 7, paragraph 1(e) of the draft RTS.

In our point of view, an intra-group due diligence has no added value. In other constellations, we would like to point out that many pension service providers are subject to strict supervision by the pension funds themselves and by NCAs or other competent authorities. Such pension funds and pension service providers also regularly have contractual agreements about the performance of audits, such as ISAE 3000a and 3402 or corresponding standards issues by national institutes of public auditors (in Germany the IDW) audits by external third parties. We therefore request to remove the internal due diligence obligation.

Question 6: Is article 8 appropriate and sufficiently clear? **(Yes)**

PensionsEurope thinks that Article 8 is appropriate and clear as rules to prevent conflict of interest are a common practice within the pension sector.

Question 7: Is article 9 appropriate and sufficiently clear? **(No)**

Article 9 regarding contractual clauses could create uncertainty for pension funds. The interpretation of how the themes of Article 30 (2) and (3) DORA related to key contractual provisions should be incorporated into clauses is likely to lead to complicated discussions between the financial entity and its ICT third-party service providers.

Thus, we would suggest the ESAs to establish standard provisions for Article 30 (2) and (3) DORA as the Commission did for data processing agreements which would save financial entities costs, negotiating time, and efforts.

We also believe that Article 9 paragraph 3 (h) is inappropriate as IT suppliers could refuse the right to audit and agree only to give information related to their certification. In those cases, we suggest certification by an external independent professional to be sufficient as it is difficult to be compliant with the requirement arising from paragraph 3 (h) for contracts related to ICT third-party providers.

Furthermore, the ESAs also require the use of independent sources to evaluate the ICT third-party service provider. While we recognise the added value of this principle which is being used in most cases for pension funds, it is occasionally difficult to find publicly independent assessments. We therefore believe that this principle should be applied on a voluntary basis as the cost of doing an independent review of ICT third-party service providers would ultimately fall on IORPs which are often small structures. The latter can instead proceed to an in-house review.

As recognised by DORA at Recital 21, pension funds outsource most of their core activities which leads pension service providers to perform a review of ICT third-party service providers. Therefore, we think they are capable of a sufficient level of assurance.

Question 8: Is article 10 appropriate and sufficiently clear? (No)

Article 10 is relatively appropriate and sufficiently clear. Indeed, the monitoring of contractual arrangements is a common practice within most of the pension sector. However, as pension funds outsource most of their core activities as recognised by recital 21 of the level one regulation, the draft RTS would imply a major change for pension funds which would be required to do this monitoring internally. To comply with level one regulation, it would be helpful if pension funds could outsource this monitoring to their main ICT third-party service providers.

Furthermore, the ESAs also require the use of independent sources to evaluate the ICT third-party service provider. While we recognise the added value of this principle which is being used in most cases for pension funds, it is occasionally difficult to find publicly independent assessments. We therefore believe that this principle should be applied on a voluntary basis as the cost of doing an independent review of ICT third-party service providers would ultimately fall on IORPs which are often small structures. The latter can instead proceed to an in-house review.

Pension funds outsource most of their core activities. DORA Recital 21 points at this practice. That means that pension service providers perform a review of ICT third-party service providers. Therefore, we think they are capable of a sufficient level of assurance.

Finally, it is also key to clarify how often ICT Third-party services providers must be audited in the light of paragraph 2(b) which lacks details on the involvement of internal auditors and at what stage.

Question 9: Is article 11 appropriate and sufficiently clear? **(No)**

Article 11 introduces a good practice to be implemented for the exit and termination of contractual arrangements. However, it could be better defined to consider practices of pension funds which often outsource managing ICT third-party providers to their main ICT provider or processor as it recognised by recital 21 of DORA. Therefore, the draft RTS should rather allow pension funds to delegate this task to the main ICT providers to avoid destabilising the relationship between pension funds and the main processors.

Article 11 should also provide more details regards the extent to which the documented exit plan shall be set up for each contractual arrangement and each ICT service assessing each ICT service separately.

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 4 other European countries[1].

PensionsEurope member organisations cover different types of workplace pensions for over **110 million people.** Through its Member Associations PensionsEurope represents **€ 7 trillion of assets**

[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.

managed for future pension payments. In addition, many members of PensionsEurope also cover personal pensions, which are connected with an employment relation.

PensionsEurope also has **20 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

PensionsEurope answer regarding the ESA's consultation on Draft ITS on register of information

Joint European Supervisory Authority Consultation paper on DORA

September 2023

www.pensionseurope.eu

Question 1: Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?

Overall, PensionsEurope acknowledges the importance of registering and reporting ICT agreements but the draft ITS is not proportionate and requires an overwhelming effort for Financial entities (FEs) to develop comprehensive registers and manually populate extensive taxonomy. In other words, the benefit-to-cost ratio between strengthening the digital operational resilience within the financial sector and the administrative burden put on the FEs is skewed.

Moreover, the proportionality principle is not sufficiently enshrined in the draft ITS. Indeed, the assertion that a financial entity "[FE] relying on a significant number of ICT third-party service providers has more information to report in the register of information than an FE depending on a small number of ICT third-party service providers" does not adequately reflect the proportionality principle.

The approach in applying the proportionality principle should rather be risk-based, meaning that higher-risk financial entities should be required to maintain a more comprehensive register, while lower-risk entities should be required to maintain a register that is simpler.

Furthermore, considering the overwhelming task for FEs to develop comprehensive registers and manually populate extensive taxonomy as well as the reliance on third parties makes it important for the FEs to have sufficient time to implement the register. In our view, FEs need at least two years from the date of application to implement the requirements

The requirement to procure and maintain an LEI for the ICT service provider must be adequately enforced by national competent authorities to avoid the situation where such a provider that is considered as "not substitutable" does not procure an LEI after a request from financial entities such as IORPs.

Moreover, a LEI number is only an obligation for some types of financial entities. ICT services providers often do not have a LEI number. Our suggestion is to also make it possible to use the registration number of the chamber of commerce.

Finally, we also want to highlight that ICT TPPs located outside the EU generally do not have a LEI, meaning it is also important to allow for other identification sources, such as a VAT-number.

Question 2: Do you agree with Article 4(1)that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?

We generally support the ESA's objective of having a holistic risk-based view of the ICT service supply chain by compiling data on "material" subcontractors. However, the granularity of the data required will make it difficult to compile on already existing outsourcing agreements and would lead to ineffective reporting requirements.

There should be a reasonable limit to the rank of subcontractors which needs to be logged, presumably rank 2 or 3. There could be disproportionate costs involved, and it would be too burdensome to require information on subcontractors of rank higher than two or three.

This is because such detailed information is often not publicly available. For instance, while it might be publicly known that a vendor is using the AWS cloud, the exact name and registration details of the relevant AWS entity may not be accessible.

Furthermore, to ensure a smooth implementation of the draft ITS, the number of mandatory data fields for these pre-existing arrangements would need to be reduced in addition to longer transition periods to allow enough time for procuring the data. We like to clarify and amend that the scope is limited to such subcontractors who render services with material ICT security risks (material subcontractors) to avoid disproportionate costs when implementing the register of information.

A solution to consider in relation to easing the administrative burden on the FEs connected to the requirement to include information on all the material subcontractors when an ICT service provided by a direct ICT TPP is supporting a critical or important function of the FEs in the respective FEs registries would be to provide the FEs with an option of working based on third-party certifications. This certification-based approach would be in line with *'Guideline 11 – Access and audit rights'* in *EIOPA's Guidelines on outsourcing to cloud service providers*. Thus, in the guideline, it reads that:

"42. Without prejudice to their final responsibility regarding the activities performed by their cloud service providers, in order to use audit resources more efficiently and decrease the organisational burden on the cloud service provider and its customers, undertakings may use:

a. third-party certifications and third-party or internal audit reports made available by the cloud service provider;"

Such an option would allow for upholding high standards for digital operational resilience, but without overburdening the FEs with administrative tasks.

Question 3: When implementing the Register of Information for the first time:

- What would be the concrete necessary tasks and processes for the financial entities?
- Are there any significant operational issues to consider?

Please elaborate.2.

PensionsEurope would like to highlight that IORPs are likely to face an over-proportional burden when implementing the register of information for the first time as IORPs usually have small structures with few human resources and are closely associated with sponsoring employers having their own IT infrastructure. As prescribed by the draft ITS, it is very time-consuming to implement the register which requires changing existing infrastructure, inventory processes, and tools. Considering the complexity and the scale of compiling such granular information, implementing such a register by January 2025 as required is not feasible.

Furthermore, Member States such as Germany and the Netherlands already have existing regulations requiring reporting of IT services with different specifications. Then, the draft ITS would change processes at the national level. Filling the proposed templates would therefore be overly time-consuming for IORPs and difficult to assess for supervisors.

As an alternative approach, To ensure a more proportionate operational burden in filling in the register, the contractors and suppliers should be able to self-register centrally so that no customers using the contractor and supplier are required to do this individually.

Finally, another reasonable compromise in line with the proportionality principle would involve creating registers for non-critical ICT services with less information, limited to essential details like service provider identification, the category of the ICT service, and the financial entity using the service.

Question 4: Have you identified any significant operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information?

The level one regulation only foresees in Article 8 (3) that "financial entities shall use state-of-the-art ICT technology (..) which (..) ensure that data is protected from poor administration or processing-related risks, including inadequate record-keeping". There is no evidence shown by the ESAs to understand properly the rationale of the five-year threshold, but it is similar to requirements arising from tax legislation. Furthermore, the draft RTS should also consider rules on data protection which require that recorded data is limited to what is deemed necessary which could lead to a lower granularity. We would also like to ensure that such a requirement for keeping information is not retroactive to avoid seeing its application to terminated contracts.

Indeed, the registration of terminated contracts as planned by the draft ITS does not have added value for ensuring sound monitoring of ICT third-party risk in the financial sector as mandated by the DORA framework. A terminated contract would not cause any risk to the financial sector.

Question 5: Is Article 6 sufficiently clear regarding the assignment of responsibilities for maintaining and updating the register of information at sub-consolidated and consolidated level?

As a matter of efficiency, when financial entity A procures ICT services from financial entity B it appears highly redundant to require each of the entities to repeat the full set of chain information on their own register. It would be easier for national competent authorities to enforce reporting rules while fulfilling its objectives if Entity A is allowed to refer to the information register of Entity B.

Furthermore, we would like to point out that Article 7 of the draft ITS also has important consequences regarding responsibilities for maintaining the register for information as it makes the financial entity solely responsible for the accuracy of the register. Indeed, Article 7(c) prescribes *"that the information recorded in the register of information is accurate and consistent over time with the information maintained and updated in the registers of information at entity level by the entities forming a consolidated or, where relevant, sub-consolidated group. Financial entities shall promptly correct any errors or discrepancies between all affected registers of information maintained by the financial entities within the scope of sub-consolidation and consolidation".*

A financial entity cannot be entirely responsible for the correctness of the register as they are relying on the information that direct ICT third-party service providers communicate to their subcontractors. In their register, incorrect information on ranks 2 and 3 can therefore be provided or the financial entity would have to look for the subcontractors used by their direct third-party service providers. It is also possible in the latter case, this information is not available.

Question 6: Do you see significant operational issues to consider when each financial entity shall maintain and update the registers of information at sub-consolidated and consolidated level in addition to the register of information at the entity level?

As mentioned above, in our answer to question 5 we see a risk of redundancies with the financial entity having to fulfil registers of information at multi-levels. Sufficient time would also be needed for financial entities to ensure a proper flow of information in case of pre-existing contractual arrangements.

Question 7: Do you agree with the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) in the template RT.02.01 on general information on the contractual arrangements? If not, could you please provide a clear rationale and suggest any alternatives if available?

Such a level of detail would be difficult to provide for IORPs when services are procured from a sponsor company. In those cases which are not rare, the ICT services could be bundled with other administrative support services. Then, the dedicated cost of ICT services might not be separately disclosed in the contract.

Question 8: Do you agree that template RT.05.02 on ICT service supply chain enables financial entities and supervisors to properly capture the full (material) ICT value chain? If not, which aspects are missing?

As mentioned in our answer to question 2, we generally support the ESAs objective of having a risk-based view of the ICT service supply chain. However, we believe the draft ITS is not proportionate as it has no limits for the depth or length of a supply chain. Each additional level of the supply chain to be reported is increasing the burden for financial entities.

We are reiterating that the required disclosures on material subcontractors in case of critical or important functions should be put only to rank 2. Indeed, the financial entity's influence on the material subcontractor is very low. Furthermore, instead of focusing on the high investment spending in ICT services which the register of information seems to prioritise, the quality of the ICT services should be the primary target of ESAs and national competent authorities.

In addition, while GDPR-related practices have prompted ICT service providers to make information on subprocessors (rank 2) publicly available, this standard aims to cover not only subprocessors but also any subcontractors, adding additional complexity to the reporting process. It may result in manual requests, especially in cases of standard SaaS where financial entities may have no direct contact for such reporting. Moreover, information on subcontractors beyond the second rank may not be available even to the direct ICT service provider itself.

Considering these challenges, we strongly recommend aligning this reporting requirement with established GDPR practices and limiting it to subcontractors involved in processing personal data, including those handling encrypted personal data (e.g., hosting service providers), thus covering all major risks. By focusing on these critical aspects, the reporting process would be more practical, relevant, and consistent with existing data protection measures]

Question 9: Do you support the proposed taxonomy for ICT services in Annex IV? If not, please explain and provide alternative suggestions, if available?

In general, the taxonomy used throughout the ITS is woolly, which makes it unnecessarily difficult for the FEs to implement the requirements.

Furthermore, since regulatory consistency across jurisdictions (beyond the EU context) is currently lacking, the proposed taxonomy should contribute to achieving an aligned approach, also granting clarity for all third-party and ICT services.

In continuation of the above, we would encourage the ESAs to provide clear definitions of key terms used in the ITS.

Furthermore, Annex IV is too extensive and should be limited to exclude elements that cannot be considered ICT services. The level one regulation at Article 3 (21) defines ICT "services as *digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services*."

ICT services such as network materials (S12) or hardware rental (S13) as the renting entity still retains control over the rented hardware should be excluded from the taxonomy as well as software licensing (S1), business analysis (S2), physical onsite security (S8) and ICT consulting (S16) because they are not matching the level 1 definition of ICT services. Moreover, both S2 and S16 do not rely on ICT systems.

Finally, the taxonomy should also include the functioning of a server room as we consider it to be in line with the definition of an ICT service. It could fall under network services (S15) as the air conditioning of the server room is needed for its operations. However, to avoid capturing ancillary services in and around the server room such as the physical cleaning of the server room, the S15 should be better defined to have a more limited interpretation of network management services.]

Question 10: Do you agree with the instructions provided in Annex V on how to report the total value of assets and the value of other financial indicator for each type of financial entity? If not, please explain and provide alternative suggestions?

For IORPs, annex V refers to a 2021 ECB guideline requiring assets to be reported at market values. This would lead to an extra burden for them where statutory balance sheets use a different method of valuation. Continuing to use existing statutory balance sheets would be the best option for IORPs since the added value of providing data on assets at market values for the DORA reporting requirements is not high since it seems that the number is used to identify the relative magnitude of the reporting unit and would not be used to prepare any exact comparisons or aggregations.

Question 11: Is the structure of the Register of Information clear? If not, please explain what aspects are unclear and suggest any alternatives, if available?

The level of detail required under the register of information is very high given the numerous templates to be filled in. It is unlikely that this would lead to clarity both for financial entities and for supervisors as

the structure of the draft ITS is overly complicated. We would advocate for limiting the registered information to key data which suffice to identify the inherent major risks while keeping the amount of data manageable with an overview.

Question 12: Do you agree with the level of information requested in the Register of Information templates? Do you think that the minimum level of information requested is sufficient to fulfill the three purposes of the Register of Information, while also considering the varying levels of granularity and maturity among different financial entities?

[The approach adopted is not proportional and the varying criticality of the FEs' individual system and functions are not taken into consideration. Furthermore, it remains unclear what tangible benefits such comprehensive information would yield.

Therefore, we propose that the ESAs go through each information point in the templates and assess whether they are strictly necessary, taking into account both benefits and costs, and if they are covered by the mandate given to the ESAs pursuant to Article 28.9 of DORA.

A more balanced approach in line with the proportionality principle would be to employ less extensive templates for ICT services that are not supporting critical or important functions. By tailoring the templates based on the level of criticality, the regulatory burden can be mitigated for less impactful services, while still capturing necessary information for services of higher importance to operational resilience.

Furthermore, the required level of information requested is likely to generate a risk of reporting mistakes which would not help national competent authorities to get an overview of the ICT dependencies of financial entities. When implementing the DORA reporting requirements and to tackle the lack of proportionality of the draft ITS, competent authorities should follow a gradual approach to ensure ownership of the new reporting rules by financial entities.]

Question 13: Do you agree with the principle of used to draft the ITS? If not, please explain why you disagree and which alternative approach you would suggest.

The principle underpinning the draft ITS is not in line with the DORA Level 1 mandate. It also imposes unduly and burdensome obligations on financial entities. While recognising the importance of registering and reporting ICT agreements, the ITS as it currently stands requires a disproportionate effort to develop comprehensive registers, manually populate an extensive taxonomy, and ensure the continued monitoring and review of this data. We would favour a more realistic, risk-based, and proportionate approach.

Question 14: Do you agree with the impact assessment and the main conclusions stemming from it?

In addition to the consultation questions above, for each column of each template of the register of information, the following is asked:

a) Do you think the column should be kept? Y/**N**

b) Do you see a need to amend the column? **Y**/N

c) Comments in case the answer to question (a) and/or question (b) "No".

PensionsEurope already expressed critical feedback on some of the columns such as in our answer to question 7 on the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) or in our answer to question 8 on the number of ranks to be considered in subcontracting constellations.

We are sceptical regarding the positive cost-benefit assessment that the register would be of benefit to the financial entities. The management of financial entities already has good knowledge of the contractual arrangements of the latter and the associated risks. Therefore, as the implementing costs of the register of information are very high, we doubt it would bring substantial added value for financial entities and for supervisors.

We signal a challenge that the contract register becomes very large. There would be too much sensitive information from too many different disciplines at one place and it would be a challenge to keep the information separate and secure with a lot of different access roles. We see a risk with a lack of clarity and responsibility and the protection of confidential information.]

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 4 other European countries[1].

PensionsEurope member organisations cover different types of workplace pensions for over **110 million people.** Through its Member Associations PensionsEurope represents **€ 7 trillion of assets** managed for future pension payments. In addition, many members of PensionsEurope also cover personal pensions, which are connected with an employment relation.

PensionsEurope also has **20 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;

[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.

- 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