AEIP input to joint consultation on the first batch of DORA policy products

September 2023

European Association of Paritarian Institutions - AEIP

1. Consultation on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

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.

AEIP acknowledges the significance of a robust governance and risk management system to preempt and mitigate the consequences of ICT-related incidents and threats. We extend our support to DORA and its mission to establish a comprehensive digital operational resilience framework for the financial sector. Nevertheless, we wish to highlight our concerns from the perspective of the paritarian occupational pension funds.

We believe that this regulation fails to consider numerous – unique - specificities of the pension sector and does not incorporate the principle of proportionality in an adequate manner. Pension funds are not typical financial market participants (the social purpose of a pension fund differentiates it from other financial entities, see recital 32 of IORPII). The landscape of IORPs throughout the EU exhibits significant diversity concerning factors such as scale, pension scheme types, social and labor laws, institutional structures, and contractual obligations. If legislators wish to make horizontal legislation for the entire financial sector, they should regard the specificities of pension funds by allowing room for adapted implementation.

Pension funds, are "not-for-profit" entities. They do not have shareholders, and their operations do not involve the sale of commercial products, as affiliation with these funds is frequently compulsory for employees due to their employment contract. Supplementary pension schemes typically adhere to a collaborative model, established and overseen jointly by social partners. Consequently, many of the recommended measures may not effectively contribute to the intended risk mitigation for pension funds. DORA should align with the overarching objective of pension funds, which is to deliver a secure and prosperous retirement for their members and beneficiaries.

The accumulation phase in pension funds spans an extended period, often aligning with the entirety of an employee's career. Members generally cannot access their pension benefits before reaching retirement age. Typically, pension administration processes occur on a periodic basis, such as monthly, quarterly, or yearly, during which member data is updated accordingly. Consequently, pension funds do not operate with real-time data. This characteristic makes them comparatively less susceptible to cyber threats when compared to other financial entities.

DORA should incorporate the flexibility to consider sector-specific attributes during its implementation by permitting a risk-based and principle-based approach to its requirements. Facilitating a risk-based and principle-based application of DORA requirements within the pension fund sector serves the best interests of the European financial system. This approach entails financial entities adhering to statutory principles

and, under regulatory oversight, defining suitable control measures while providing clear explanations for their compliance with DORA.

Establishing appropriate requirements is essential to prevent pension funds and supervisors from incurring disproportionate and unnecessary costs. Our concern primarily stems from the level of detail in the provisions and the absence of proportionality in their application. Many of the prescribed control measures, in their current form, do not effectively contribute to strengthening the operational resilience of pension funds. Instead, an excessive number of control measures, if implemented in a rigid, rule-based manner, will divert the resources of pension providers and supervisors without effectively addressing the most critical risks. We believe that Art. 29 of the RTS should at the very least also include outsourcing as one of the elements that have to be taken into account. This is in line with recital 21 of DORA. Financial entities that outsource all their operational activities are required to set up an entire detailed framework while for those entities the DORA requirements should focus on managing the ICT critical or important third-party risk.

To ensure the complete implementation of proportionality as outlined in Article 15 of DORA, we advocate for each RTS to adopt a requirements model akin to widely recognized industry standards such as OWASP ASVS, NIST CSF, and other NIST "Special Publications." It is regrettable that the RTS appears to be establishing its own regulatory framework rather than referencing globally accepted industry standards. This carries the risk of introducing additional costs and uncertainty regarding whether sector-specific standards align fully with DORA compliance or not.

In AEIP's perspective RTS should be tailored to the specific characteristics of the pension fund sector, resulting in more focused and purpose-fit requirements for IORPs – with proportionate application. At last, a sufficiently extended transition period should be afforded to facilitate the effective implementation of DORA.

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.

Overall, we wish to highlight that a significant portion of the guidance contained within the various RTS and ITS consultation documents presented by the ESAs essentially transforms DORA Level I's principle-based requirements into more rigid, rule-based requirements at the DORA Level II stage. AEIP Members believe that the simplified ICT risk management framework is far too it is far too granular and prescriptive, thus negating the aim of Article 16 of DORA. We point out that in several cases, these rule-based requirements are derived from existing regulations applicable to a particular category of financial institutions (e.g., banks), which makes them ill-suited for the unique characteristics of pension funds.

With the introduction of these stricter rule-based requirements, it appears that the proportionality principle outlined in Article 4 of DORA has been significantly narrowed down. In practice, size appears to be the primary factor considered in determining proportionality, while factors such as the nature, scale, and complexity of the services, activities, and operations are no longer given due consideration.

Consequently, many of the original DORA requirements have been transformed into Level II implementation requirements that impose stricter standards than what may be necessary for pension funds (IORPs) and their service providers to achieve an appropriate level of digital operational resilience. Given the paramount importance of proportionality, it is essential that each type of financial entity establishes its own tailored 'sectoral' reference point.

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

AEIP is of the opinion that the governance provisions lack the necessary level of detail to be proportionally applied to IORPs.

The current RTS fails to make a suitable distinction between various levels of risk, and it doesn't seem logical to mandate all financial entities to undertake the same set of actions. The RTS acknowledges the financial system and its constituent entities as a collective subject to certain cyber risks but overlooks the individual nuances of these entities' ICT systems. We acknowledge that IORPs are integral parts of the financial system and are recognized as financial entities (with a social purpose), subject to DORA, the RTS, and their associated requirements. However, it is important to emphasize that we are also reliant on other financial entities that are similarly subject to these regulations. Therefore, a judicious tiering of financial entities based on their significance in the EU financial system and their interdependencies, as stipulated in the RTS, would significantly enhance the ability to address risks at the appropriate junctures instead of imposing redundant efforts on all entities solely for compliance purposes.

Focusing on actual digital resilience testing, a facet often absent in many other regulations, requirements, and international best practices, and subsequently gathering, analyzing, and sharing the results with other financial entities, could make a considerable difference with less effort. We believe that cross-industry tabletop exercises, possibly under the auspices of ENISA (European Union Agency for Cybersecurity), that simulate scenarios with systemic implications, would benefit all stakeholders in the financial industry. Such exercises could be instrumental in identifying critical interfaces between different players where the potential impact is most likely to occur, mirroring common practices in other industries.

It's important to bear in mind that it's a common practice to manage business risk comprehensively, where ICT or Cyber risk is considered a component of the broader operational risk to a business.

The RTS and its accompanying requirements exhibit significant overlap with established international ICT Security and Risk best practices, as well as with national, international, and sector-specific guidelines and regulations addressing similar topics. This overlap raises questions about the added value of DORA, the RTS, and their associated requirements, which appears to be extremely limited.

In light of this, it's worth considering whether a more sensible approach might involve referencing industry standards instead. This could potentially result in a more rational and transparent proportionality principle (see also Q.1).

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

We disagree with the proposed approach to ICT risk management policy and processes, as it appears to be impractical given that most IORPs lack in-house staff and ICT infrastructure. In many instances, the IT infrastructure is owned and operated by third-party providers or the organizers of pension schemes, who already have their own ICT risk management policies and processes in place. Moreover, the majority of IORPs do not have full-time equivalent (FTE) positions dedicated to ICT or ICT security roles.

We firmly believe that financial entities that outsource all their operational activities should not be mandated to establish an entire separate framework. Instead, DORA requirements in such cases should focus on managing critical or significant third-party ICT risks, which can be achieved through appropriate clauses in contractual arrangements with these parties. Imposing obligations like setting up a Network Operations Center (NOC)/Security Operations Center (SOC) or conducting Threat-Led Penetration Testing (TLPT) on financial entities that fully outsource their operational activities does not seem to provide meaningful added value.

Additionally, we hold the view that the requirement outlined in Article 4.2 ("ICT asset management policy") should be limited to critical ICT systems to ensure proportionality in the information required.

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

x

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?

x

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

Article 6, paragraph 2(a) stipulates that all data must be encrypted, and if encryption of data in use is not feasible, financial entities should process data in a segregated and protected environment. It's important to recognize that data encryption is indeed a control measure and should be aligned with the principles of the CIA triad - Confidentiality, Integrity, and Availability.

To ensure proportionality in risk management, there should be room for prudent decision-making regarding data encryption, especially for publicly available data and data categorized as low-risk in terms of the CIA triad. The current draft RTS, with its rigid rules-based approach, can impose unnecessarily heavy risk management requirements. At the very least, an exception should be considered for publicly available data and data that pose low risks in terms of confidentiality, integrity, and availability.

Also see our reply in Q.4.

Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No

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

See our reply in Q.4, additionally:

Article 9(1), mandates financial entities to identify the capacity requirements of their ICT systems and implement resource optimization and monitoring procedures. It's important to note that pension provision operations, particularly pension administration, often exhibit a high degree of predictability and planning. This characteristic warrants a risk-based approach tailored to the specific operational security needs of pension funds. The current drafting of the article could be considered disproportionate in the context of pension fund operations.

Article 10(2)(c) mandates ICT third-party service providers to manage and report any vulnerabilities they discover to the financial entities. While it is important to address vulnerabilities, this approach may lead to a situation where every discovered vulnerability is reported by all parties in the ICT chain. This could result in reporting overload, making it challenging to manage and assess the sheer volume of vulnerability reports. Many of these reports may be irrelevant, potentially diverting resources towards administrative tasks, and increasing the risk of overlooking and not adequately addressing serious vulnerabilities. A more streamlined and risk-focused approach to vulnerability reporting may be necessary to address this issue efficiently.

Article 10(2)(b) mandates weekly vulnerability scans for critical or important functions. While regular vulnerability scans are essential, a weekly scanning frequency could indeed impose a significant workload on IORPs (Institutions for Occupational Retirement Provision). It may be advisable to reconsider this frequency requirement for IORPs, as it may be disproportionate given the specific operational characteristics and resource constraints of these entities. Adjusting the scanning frequency to align with the operational context of IORPs could be a more practical approach.

Article 10(2)(e) calls for the establishment of a procedure for 'responsible disclosure' of vulnerabilities to clients, counterparts, and the public. It's important to consider whether this requirement is proportionate to the activities typically undertaken by an IORP. Given the nature of their operations, it may be reasonable to reassess whether such a procedure is necessary for IORPs, as it may not align with their specific functions and responsibilities.

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

Article 12, paragraph 2(c) mandates the logging of events related to access control, capacity management, change management, and network traffic activities. While comprehensive logging is essential for security, it's also important to acknowledge that excessive logging can generate a significant number of false positives. Researching them requires a lot of man-hours, which then cannot be deployed on other essential

issues. This activity risks being seen as unnecessary administration. The option to apply professional judgement would improve the adaptation of this requirement.

Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No

What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.

Weekly vulnerability scans for all ICT assets are already common practice with pension funds. We therefore foresee no impact of this measure. See also our reply in Q.4.

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.

Article 11.2(k) concerning "cloud computing resources" may not fully align with how cloud technologies are commonly utilized in practice. In many cases, the "cloud client interface" is not initiated manually by an individual but rather through automated processes supported by technologies like "Infrastructure-as-Code" or as an integral part of a Continuous Integration/Continuous Deployment (CI/CD) pipeline in the context of software development and deployment.

Considering these modern practices, it would be beneficial to amend this point accordingly to reflect the evolving landscape of cloud technology usage. Furthermore, as previously mentioned, it could be advantageous for Article 11 to reference relevant existing standards and guidance, particularly those that are open source or open licensed, to ensure alignment with established industry best practices and facilitate compliance.

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

See our reply in Q.4, also:

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

Article 13(1)(c): Depending on the interpretation of the prohibition of direct internet access from devices or servers used for information system administration, it will be difficult to perform system updates as these are only available online.

Article 13(1)(h): The review of firewall rules and connections filters should be performed on a yearly basis. The modification of these rules for ICT systems supporting critical or important functions are not frequent enough to justify a six-month basis. The review is made in the phase of the project if there are rules to be changed.

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.

AEIP recommends including the possibility of multi-factor authentication (MFA) as an option in certain cases within the RTS. Considering that a significant majority of cyberattacks today commence with the compromise of end-user credentials, it's crucial to explicitly reference MFA in the RTS. Doing so will help financial entities recognize it as a primary defensive measure for bolstering security and reducing the risk of unauthorized access.

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

We share the concern that the prescribed approach to project and change management in the RTS may hinder the adoption of modern development methodologies, such as Agile working. These approaches promote flexibility, iterative development, and rapid change, which may not align seamlessly with the more rigid project and change management requirements outlined in Article 16.

Additionally, Article 16, paragraph 4, which introduces a requirement for source code review, may present challenges. ICT third-party providers may be reluctant to make all source codes available to financial entities, and conducting such reviews may not align with the expertise or operational focus of pension funds.

In light of these considerations, it could be beneficial to explore alternative approaches that allow pension funds to rely on cybersecurity product quality assurances, while also adhering to EU digital contract rules, to ensure effective cybersecurity without imposing undue burdens.

Moreover, the RTS approach on ICT project management is dated by (only) taking projects into account as monolithic projects spanning several months and even years, while nowadays we are used to apply test-driven approaches that are much smaller in scope, and impact. By imposing these obligations on such projects, we believe that financial entities of all sizes will incur higher costs for their development, maintenance, and acquisition projects. It would be useful if the RTS applied proportionality based on the project's classification. There should be a more pragmatic attitude based on cost, risk and potential impact.

Similarly, the suggested approach on ICT change management should also integrate proportionality and adopt a more pragmatic attitude.

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 believe that existing industry standards and regulation already provide sufficient guidance. The requirements regarding supply-chain risk, risk to be superfluous.

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

x

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

We believe the suggested approach should be in line with existing industry standards and regulation.

Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No

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

See our reply in Q.4.

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

See our reply in Q.4.

Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

No.

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.

See our reply in Q.4.

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

Article 27(2) outlines a specific set of scenarios to be identified, and it's important to consider that an excessive amount of scenarios, especially those that are not relevant or have an extremely low probability of occurrence, could indeed diminish the value of this measure. To ensure the effectiveness of this requirement, it would be prudent to focus on scenarios that are genuinely relevant to the specific financial entity in question. An approach that tailors the scenarios to the entity's nature of operations, risk profile, and potential threats would be more practical and cost-effective. This approach would help avoid staff

unwillingness to comply, reduce unnecessary paperwork, and minimize associated costs while still addressing meaningful risk scenarios. Also see our reply in Q.4.

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

x

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.

No. In line with our response to Question 4, we believe that the suggested approach on the format and content of the report, is far too detailed and prescriptive given the limited risk profile of IORPs. Article 28 is very prescriptive in format. It would not allow pension funds to attune to the most relevant aspects for the sector. Currently used formats would no longer be allowed. That would negatively impact the helicopter view of pension fund board members.

Moreover, in practice it will be nearly impossible to apply certain requirements given the fact that most IORPs do not have own staff and ICT infrastructure. Furthermore, Article 6(5) mentions that the report should be provided on an ad hoc basis to the competent authority. However, the RTS is extremely specific in the format of the report and its contents. Much of the information mentioned would be useless to any reader without further internal context. We believe that the competent authorities would benefit much more from a less detailed, roll-up report indicating the exposure of specific financial entities to areas of risk relevant to the broader European financial system. We believe that a more risk-based approach would be beneficial.

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

Reiterating our answers to Question 1, 2 and 4, we do not believe that IORPs - which often do not have own staff and/or ICT resources, would benefit from the simplified ICT risk management framework as described in the RTS. Therefore, we cannot agree with it as such. We believe that a more risk-based approach would be beneficial acknowledging the risk ownership proportionate with the position and potential impact of a financial entity on the broader European financial system.

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.

See our reply in Q.4.

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.

As mentioned in our response to Question 4, IORPs often do not have own staff and/or ICT resources. An expansion of the ICT operation security requirements for all ICT assets, which is covered for all entities in

both industry good practices as well as industry-specific regulation would be superfluous and risks to increase the burden on ill-defined smaller financial entities without improving the overall risk profile of the European financial sector.

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.

x

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.

See our reply in Q.4.

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.

See our reply in Q.4.

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

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.

Yes / No

We believe that DORA and the RTS does not sufficiently recognize the distinct nature of the activities performed by pension funds given that they are 'not-for-profit', seldomly work with real time data and as a rule perform the pension administration process on a periodical basis (monthly, quarterly or yearly). Some of the proposed criteria by the RTS are therefore less appropriate for pension funds to ascertain whether a certain occurrence constitutes as an incident or not. This is mainly due to the fact that pension funds are established by a limited number of sponsoring undertakings (in some/most cases there is only one sponsoring undertaking) and that pension administration processes are done on a periodical basis (monthly, quarterly or yearly). Specifically with regards to pension funds that operate on a cross-border basis it should be noted that the criterion of 'geographical spread' risks to lead to overreporting.

In order to adequately incorporated proportionality for pension funds we would therefor suggest not to take the criterion of 'clients, financial counterparts, and transactions affected' as a primary criterion, thus

limiting the primary criteria to 'data losses' and 'critical services affected'. Secondly, the secondary criteria need to be interpreted in a sector/entity-specific manner. Precisely:

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

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

We do not consider Clients, financial counterparts and transactions affected to be a primary criterion. This criterion has been designed in a way that many incidents at big financial entities satisfy this criterion. The ESAs suggest an approach where an incident is classified as major when at least one primary and two secondary criteria are met. With clients, financial counterparts and transactions affected as a primary criterion, that means many incidents that are not material to the financial entity or it clients will nevertheless be reported as major, creating 'false positive' reports that also require processing by the supervisor.

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

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

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

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.

Yes / <u>No</u>

We have significant apprehensions that, given the existing specifications and thresholds, a considerable number of incidents could be wrongly categorized under this criterion for numerous pension funds.

DORA Recital 21 emphasizes the importance of competent authorities adopting a vigilant yet balanced approach when supervising institutions for occupational retirement provision. These institutions often delegate a substantial portion of their core business functions, such as asset management, actuarial calculations, accounting, and data management, to service providers. It's crucial that this close relationship is duly considered and taken into account when applying delegated acts.

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

An alternative recommendation for this criterion could involve the implementation of a unified approach, wherein both the pension fund and its service provider are viewed as a single entity. This approach would acknowledge the close relationship between the pension fund and the service provider, aligning with the principles outlined in DORA Recital 21. The assessment criterion, which considers clients, financial counterparts, and affected transactions, would be applied to the pension fund as the ultimate client of the service provider. The adoption of the consolidated approach could be structured as a conditional provision, allowing the pension fund and its service provider to employ this method only if they can substantiate its effectiveness.

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

Concerning the impact on relevant clients or financial counterparts, we reference DORA's Recital 21, which outlines that IORPs often delegate a significant portion of their core functions, such as asset management, actuarial calculations, accounting, and data management, to service providers. In light of this, it is our contention that this criterion should not be applied to the service provider of the pension fund. The service provider's role is of such paramount importance to the pension fund that any disruption would have a direct bearing on the achievement of the pension fund's aims and objectives.

Many pension service providers provide a standard service to a limited number of pension funds. Pension funds are rather simple organizations that usually execute a single product/service – the pension scheme – to all of it members and beneficiaries. That means that the absolute and relative thresholds for clients affected will be affected just as well. We would therefor suggest that the different aspects of this criterion would not be treated separately and as alternative triggers for incident reporting, but instead would be viewed globally and interpreted in an sector/entity-specific manner which specifically for pension funds would entail that in practice only the sub-criterion 'clients' and 'relevance of clients' would come into effect.

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.

Yes / No

Duration and service downtime

We do not agree with the ESA's interpretation that either 'service downtime' or 'duration of an incident' should be able to trigger this classification criterion. Article 18(1)(b) of DORA refers to "the duration of the ICT-related incident, including the service downtime", thereby clearly stating that the occurrence of a service downtime is a prerequisite for an incident. If there is no service downtime, this criterion cannot be triggered.

A fundamental characteristic of pension funds is the periodic nature of their activities, wherein pension entitlements are disbursed on a monthly basis. Administrative and transaction systems are effectively active only on specific days of the month. We believe that service downtime should be defined as those hours during which systems supporting critical or important functions are actively in use or "online." If a service does not need to be operational at a particular time, it would not be logical to consider it as being "down." It should be interpreted in an sector/entity-specific manner. We believe that in the context of IORPs, a duration of 24 hours is too short and that a longer period of time should be taken into consideration. Finally we are wary of any double use of certain criteria. Beyond the hours when systems supporting critical or vital functions are actively utilized, the duration of an incident should not be categorized as service downtime. During such times, the availability, authenticity, integrity, and confidentiality of pension data may still be at risk, but these specific aspects are already addressed within the data losses criterion.

Reputational impact

This criterion fails to adequately account for the unique nature of pension funds and their operations, as some elements of this criterion are not applicable to pension funds. For instance, the potential loss of clients or financial counterparts, which translates to the potential loss of members or sponsoring undertakings, is not a suitable criterion for pension funds. This is because sponsoring undertakings typically establish the pension fund as a distinct legal entity, and members usually lack the ability to choose an

alternative pension provider. Consequently, the various aspects of this criterion should be assessed collectively and interpreted in a manner specific to the sector or entity.

Regarding the threshold, we believe that any impact, without further specification, poses the risk of producing undesirable outcomes. We contend that the threshold should only be triggered in the presence of a substantial or well-substantiated impact. For instance, unwarranted claims from stakeholders should not be classified as an incident.

Geographical spread

This criterion carries the potential to yield distorted outcomes for pension funds that operate on a cross-border basis. A cross-border pension fund engages in one or more cross-border activities in which the IORP is established in one European member state (the home state) and manages pension benefits for members employed by a European employer offering an occupational scheme, with the employer/employee relationship situated in another European member state (the host state). Such funds, by their nature, will have operations spanning at least two Member States. This criterion may inadvertently categorize more incidents due to the cross-border nature of their activities, while this might not have been the case for pension funds solely involved in domestic schemes. We find it challenging to discern the underlying rationale for this approach.

Economic impact

We question the materiality of the proposed threshold of 100 000 EUR. Setting the bar too low, risks to unnecessarily burden pension funds and supervisors alike. We would suggest to raise said threshold. Additionally, staff costs are difficult to calculate. Resolving ICT-related incidents is part of ongoing activities. If an incident occurs at a quiet time, no additional staff needs to be involved. In such case, there is no direct loss in staff costs. Only if an incident incurs additional staff costs on top of the budget, costs would have to be attributed to the cost of the ICT-related incident.

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.

Yes / No

We share the consensus that this is a fundamental criterion, and we endorse the details outlined in the draft RTS for defining what qualifies as 'data losses' concerning availability, authenticity, integrity, and confidentiality.

Given the importance of this primary criterion, we concur that the establishment of a threshold is necessary. Specifically, this threshold should signify a substantial impact on critical data that adversely affects the financial entity's ability to carry out its business objectives or meet specific regulatory obligations.

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.

Yes / No

As pension funds necessitate authorization, the initial aspect of this criterion will inherently pertain to pension funds. Consequently, it is imperative to assess the various components of this criterion holistically and interpret them in a manner specific to the sector or entity. This approach ensures that only incidents related to ICT services supporting critical or important functions of the financial entity are taken into consideration. Otherwise, this primary criterion would invariably be triggered for all pension funds, which may not accurately reflect the significance of the incidents.

AEIP thinks this criterion is too broadly formulated. In our view, the specification of whether an incident has affected services or activities that require authorization is not relevant enough to feature in this criterion. Many services require authorization, it seems therefore that this specification touches upon the authenticity, integrity and/or confidentiality of data, which is already covered in the criterion 'data losses'. It is not appropriate for this specification to feature in two criteria, thereby triggering two primary criteria at once. It would also be expedient to include the specifications as mentioned in the RTS in the sense that such escalation is different, and is to be distinguished from regular reporting.

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

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).

x

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.

Yes / No

We question how a pension fund that has outsourced its critical services can meet the requirements set out in Article 18(2) of DORA? A FE can only act on the information in its possession. However, in Article 17(1)(a) of the RTS there is also mention of a threat that could impact other FE, third party providers, clients of financial counterparts. The question arises how a FE will be made aware of this fact?

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.

Yes / No

A FE will not always have access to the required information to ascertain whether the conditions in Article 18 of the RTS are met or not. We believe it may be expedient to include the possibility of some form of anonymisation in the reporting of major incidents.

3. Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

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?

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

In the introduction of these stricter rule-based requirements, it's notable that the proportionality principle outlined in Article 4 of DORA has been notably constrained. Size appears to be the primary remaining factor considered in applying proportionality, whereas factors like the nature, scale, and complexity of the services, activities, and operations are no longer taken into full account.

Consequently, a significant outcome is that many of the original DORA requirements have been translated into Level II implementation requirements that impose greater stringency than what is necessary for IORPs and their service providers to attain an adequate level of digital operational resilience.

LEI Codes are primarily required by legal entities that are involved with financial transactions or that operate within todays financial system. Most FE therefor have a LEI Code. However legal entities stemming from other sectors usually don’t. Referring to a unique national identification number should therefor suffice when no LEI Code is available.

Do you agree with Article 4(1)b 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 agree that mapping the ICT service supply chain should only be necessary for material subcontractors who provide services critical or vital to the operations. This approach can provide financial entities with valuable insights into the "in control status" of sub-contractors concerning ICT service delivery. However, it is contingent upon contracting and subcontracting parties supplying comprehensive and up-to-date information, which can enhance the control measures of financial entities.

We believe that mandating information on the ICT service supply chain for all contracts would lead to an excessive and ineffective reporting burden. Therefore, we appreciate the decision by supervisors to limit the information required to rank 1 for such contracts.

Additionally, we share the view that, considering the register's objective of encompassing the ICT service supply chain, it is reasonable to include material subcontractors of direct ICT third-parties. However, the determination of what constitutes "materiality" should remain within the purview of the financial entity in question. The financial entity is in the best position to assess whether a subcontractor should be included in the register, taking into account the principle of proportionality. A pragmatic approach, considering factors like cost, risk, and potential impact, should be applied. Furthermore, this perspective should be interpreted in a manner that aligns with the specific needs and characteristics of the sector or entity in question.

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?**

We are cautious about imposing additional reporting obligations on financial entities. The proposed register by the ESAs, appears to be considerably more comprehensive than national procedures, which could significantly increase the reporting burden on financial entities. It would be beneficial if the required information aligns with existing European-level guidelines for information registers, such as those established by ESMA and EIOPA.

Overall, it's evident that the initial compilation of the Register of Information will necessitate a substantial effort from each IORP, leading to significant costs for the entity. It's also worth noting that maintaining the Register in an up-to-date state will require a similar level of effort and incur subsequent costs.

This will especially be burdensome for medium and small sized IORPs in comparison with other larger financial entities. It is also important to note that any raise in expenditures will ultimately diminish the pension income of members and beneficiaries thus leading to a decline in the adequacy of their pensions. In this light it stems to reason that the Register should be filled out in a sector/entity-specific manner. Alternatively, a reduced format of the Register (for all financial entities) would be reasonable and proportionate.

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?

It should be made clear that the requirement to keep information regarding contractual arrangements that have been terminated for five years, only entails that the information available at the time of termination is kept “as is”. No obligation to keep the information on direct ICT third-parties on their material subcontractors up-to-date.

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

The responsibility for maintaining information on supply chains should not rest solely with the financial entity. One of the key objectives of the ITS is to comprehensively capture the ICT service supply chain, with a specific focus on subcontractors of ICT services that support critical or important functions or material components thereof. In this context, Article 7(c) of the regulation stipulates that the information recorded in the register of information must be accurate and consistent over time with the information maintained and regularly updated in the registers of information at the entity level by the entities comprising a consolidated or, where applicable, sub-consolidated group. Financial entities are required to promptly rectify any errors or discrepancies that may arise between all affected registers of information maintained by the financial entities within the scope of sub-consolidation and consolidation.

This makes the financial entity responsible for the accuracy of the register. However, financial entities rely on the information that direct ICT third-party service providers provide on their subcontractors. A financial entity could therefore have incorrect information in their register on rank 2 and rank 3 subcontractors. Or it would have to research the subcontractors used by their direct third-party service providers. In the latter case, that information might not be available.

It could be made clear in the ITS, for example in its recitals, that financial entities can contractually delegate the responsibility for maintaining and updating the register to the direct ICT third-party service provider for information on rank 2 and further down the ICT service supply chain.

Additionally, Article 6 is not particularly applicable to AEIP Members given the fact that IORPs are not part of a group. Only the entity specific Register will apply to pension funds.

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 entity level?

x

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?

If these extra fields have to be included in the contract register, the challenge is 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. It would be hard to make one person responsible for the entire register to be correct and up-to date. We also doubt if there would be suppliers who could provide a register that meets all requested requirements, including consolidation and sub-consolidation requirements and role based access to

different information. We see the greatest risk in the area of lack of clarity and responsibility and the protection of confidential information.

Moreover, T.02.01.0041 and RT.02.01.0042 do not seem relevant in the context of a risk management approach. The annualized value of a contract is not necessarily related to the role that an ICT third-party provider plays in the value chain of a financial entity.

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?

RT.05.02 duplicates certain information from RT.05.01 while each entry in RT.05.01 could be augmented with a list representing the values in RT.05.02.0010 creating an equally high-signal link between ICT third-party providers in the same value chain.

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

The extent of ICT services should be limited. In the register, financial entities are required to identify all their operational and business and to identify the ICT services provided by ICT third-party service providers supporting the functions. It is unclear to what extent a certain function needs to be included in the register.

DORA 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."

In our view, the functioning of a server room falls under the definition of an ICT service and should be included in the register. For example, the air conditioning of the server space is relevant to its well-functioning. But ancillary services in and around the server room should not fall under the definition. For example, the physical cleaning of the server room. Services that do not directly involved ICT hardware and/ or software should not be in the remit of DORA. If they would be included, this would significantly increase the number of registered parties. At the same time, the costs of registration would not improve operational resilience.

Annex IV gives a list of ICT services. The example mentioned above could fall under S15 (network services), but it is unclear what 'management' in S15 entails. A more detailed definition, giving a limited interpretation of network management services, excluding non-ICT services in and around the server room, would be welcome.

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?

X

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

x

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?

See our answers to question 7 and 8.

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.

This question is not sufficiently clear. Therefore we cannot agree or disagree with it.

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

The current size of the register of information is too big. That makes is unworkable in practice. We suggest that the number of columns should be reduced.

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

- **Do you think the column should be kept? Y/N**
- **Do you see a need to amend the column? Y/N**
    - **Comments in case the answer to question (a) and/or question (b) "No".**

4. Public consultation on draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?

Yes / No

As a general comment, it should be noted that a large part of the guidance provided in the different RTS and ITS consultation documents presented by the ESAs, effectively results in a translation of DORA Level I principle-based requirements into DORA Level II rule-based requirements. Furthermore, these rule-

requirements are based in several instances on existing requirements for one specific category of financial institutions (e.g. banks), which means they are ill-fitting for pension funds.

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

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

Overall, we do not agree with the approach followed to incorporate proportionality. We believe that DORA and the RTS do not sufficiently recognize the specific nature of pension funds:

- pension funds are 'not-for-profit', membership is as a rule mandatory and pension schemes are mostly set up by social partners;
- pension funds seldom work with real time data: as a rule the pension administration process is done on a monthly, quarterly or yearly basis;
- pension funds have limited own ICT infrastructure and staff (often they do not even have their own personnel); so they use sponsor resources and outsource (sometimes all of) their operational and investment services.

Thus, we considerate it to be crucial that the specificities of IORPs would be reflected more in the DORA and RTS requirements and that pension funds could benefit from a more proportional treatment in this context, thus not jeopardizing the societal goal of IORPs to provide an adequate pension income for their members and beneficiaries. The lack of consideration for our organizations risks to significantly imperil the viability of the majority of IORPs across Europe.

Article 1 of the RTS should therefore at the very least also include outsourcing as one of the elements that have to be taken into account. In more general terms we believe that the RTS should be sector-specific rendering the requirements more concise and fit-for-purpose with regards to IORPS. Finally it should be noted that Article 2 of the RTS does not apply to IORPs given that they are not part of a Group.

Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

Yes / <u>No</u>

Article 3 is sufficiently clear but not appropriate given that most IORPs do not have own staff and ICT infrastructure. Typically, the IT infrastructure is under the purview of a third-party provider or the entity organizing the pension scheme. IORPs should be permitted to meet the requirements in a manner that accommodates these circumstances. Furthermore, it's important to consider that the prevailing approach often involves managing business risk comprehensively, where ICT or Cyber risk is viewed as just one component within the broader context of operational risk for a business. As a result, it might be prudent to revise the policy at intervals of at least every three years, rather than the current annual requirement.

Is article 4 appropriate and sufficiently clear?

Yes / No

We believe that the criteria mentioned in Article 4 can be used to introduce more proportionality.

Is article 5 appropriate and sufficiently clear?

Yes / No

The requirements related to managing contracts and third parties throughout the duration of the contract, along with the need for a 'Know your customer' process, are indeed sound practices. However, the mandatory requirement to establish this process can be deemed ineffective within the pension sector, given that pension funds frequently delegate the management of third-party providers to their primary processor or ICT provider. DORA's Recital 21 underscores the importance of respecting this practice by pension funds.

It would be beneficial if the responsibility for contract and third-party management could be delegated to the main processor, especially considering that they are often the primary focus of this process within the pension sector. This adjustment would streamline the regulatory framework and align it more closely with the practical operations of pension funds and their service providers.

Overall, the RTS should be interpreted in a sector-specific manner rendering the requirements more concise and fit-for-purpose for IORPS.

Are articles 6 and 7 appropriate and sufficiently clear?

Yes / No

Article 6 is clear and appropriate. Such a risk assessment is considered good practice, and already a practice within most organizations within the pension sector. We have no further comments concerning this article.

Article 7 appears to be reasonably clear and partly appropriate. Conducting a Due Diligence assessment before entering into a contract with a third party is a common practice in the pension industry and would entail minimal adjustments to our existing processes.

From our perspective, conducting an intragroup due diligence doesn't provide any additional value. Pension service providers are already subject to rigorous oversight by pension funds and National Competent Authorities (NCAs). Furthermore, there are contractual agreements in place between pension funds and pension service providers regarding the performance of ISAE 3000a and 3402 audits by external third parties. Therefore, we respectfully request the removal of the internal due diligence obligation.

While we understand the intent behind Article 7, paragraph 1(e) regarding ethical and socially responsible business practices, we fail to see its relevance to the operational resilience of ICT services and their providers. Consequently, we find it unsuitable for this due diligence requirement to be enforced under DORA.

Overall, The RTS should be interpreted in a sector-specific manner rendering the requirements more concise and fit-for-purpose for IORPS.

Is article 8 appropriate and sufficiently clear?

Yes / No

Article 8 is clear and appropriate. (Regulatory) measures to prevent Conflict of Interest are common practice within the pension sector. Overall, the RTS should be interpreted in a sector-specific manner rendering the requirements more concise and fit-for-purpose for IORPS.

Is article 9 appropriate and sufficiently clear?

Yes / No

We recognize that the topics to be included in contracts with ICT third-party service providers are well-defined. However, the interpretation of how the provisions outlined in Article 30(2) and (3) of DORA should be integrated into contractual clauses is likely to lead to intricate discussions between the financial entity and its ICT third-party service providers.

We therefore suggest, just as the European Commission has done regarding data processing agreements, to draw up standard provisions for DORA Article 30 (2) and (3). This can save financial entities a lot of negotiating time and effort as it is not necessary to discuss each clause separately with an ICT third-party service provider. It will thereby also save costs.

Experience shows that, in certain cases, IT suppliers refuse the right to audit and only agree to provide information about their certification. This is contrary to Article 9 paragraph 3 (h). In such cases, we consider certification by an external independent professional should be sufficient. As a small customer, it can be hard to include the requirement from Article 9 paragraph 3 sub h in the contracts of a ICT third-party services provider. In that case, it is impossible to become DORA compliant.

The ESAs mandate an independent audit report for the selection of ICT third-party service providers. While the utilization of independent sources aligns with best practices, it may not always be feasible to access publicly available independent assessments. In situations where such assessments are not readily available, conducting an independent review could entail additional resources.

We would like to highlight the option for financial entities to carry out an in-house review. Consequently, we propose that the requirement for an independent audit be made voluntary, offering financial entities the flexibility to choose whether to pursue an independent audit based on their specific circumstances and available resources.

Pension funds commonly outsource most of their core activities, a practice emphasized in DORA Recital 21. Consequently, pension service providers often conduct reviews of ICT third-party service providers on behalf of pension funds. From our perspective, these service providers possess the capability to offer a satisfactory level of assurance regarding the third-party ICT services.

Overall, the RTS should be interpreted in a sector-specific manner rendering the requirements more concise and fit-for-purpose for IORPS.

Is article 10 appropriate and sufficiently clear?

Yes / No

Article 10 is clear and appropriate. Monitoring compliance with contractual agreements is a standard practice in the pension sector. However, as previously mentioned in relation to Article 5, pension funds frequently delegate the management of ICT third-party providers to their primary processor or ICT provider. It would be beneficial if this responsibility could be delegated to the main processor, as imposing alternative measures for DORA compliance purposes could introduce unnecessary administrative burdens and potentially affect the legal relationship between pension funds and their main processors adversely.

The ESAs require the use of independent sources to assess the ICT third-party service provider. While the use of independent sources is a good practice that pension funds try to use in most cases, it is not always possible to find publicly available independent assessments. In such cases it would cost extra resources to get an independent review. We point at the possibility of financial entities performing a review inhouse. We therefore suggest making independent review voluntary.

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. In our view, they are able to provide a sufficient level of assurance.

Overall, the RTS should be interpreted in a sector-specific manner rendering the requirements more concise and fit-for-purpose for IORPS.

Is article 11 appropriate and sufficiently clear?

Yes / No

Article 11 is clear and appropriate. This is considered good practice to be implemented. However, as mentioned with regards to Article 5, pension funds often outsource managing ICT third-party providers to their main processor/ICT provider. It would therefore be helpful if this could be delegated to the main processor. Implementing alternative measures for DORA compliance purposes would result in unnecessary administrative overhead and adversely impact the legal relation between pension funds and the main processors.

Overall, the RTS should be interpreted in a sector-specific manner rendering the requirements more concise and fit-for-purpose for IORPS.

For further information please contact:

Panayiotis.elia@aeip.net

Panayiotis Elia, AEIP Policy Advisor, Pension & Financial Affairs

AEIP Disclaimer

AEIP represents the European Paritarian Institutions of Social Protection in Brussels since 1997. The association gathers 29 leading large and medium-sized social protection providers, which are managed on the basis of joint governance and equal representation by both employees and employers' organizations (the social partners) in 12 EU Member States.

AEIP represents its members' values and interests at the level of both European and international institutions. In particular, AEIP - through its working groups - deals with EU coordinated pension schemes and pension funds, healthcare, unemployment, provident and paid-holiday schemes.

Owing to the quality of its members and to the delegation of powers conferred to its Board, AEIP aims at becoming the leading body for the promotion of balanced paritarian social protection systems in Europe. AEIP promotes and develops programs and orientations aiming at the sustainability of paritarian social protection systems at local level taking into account the national specificities aiming at ensuring social cohesion in Europe.

Based thereon, AEIP prepares recommendations, proposes local programs and influences European decisions to safeguard and promote the interests of its members. AEIP thinks ahead and anticipate modern paritarian social protection systems that take into account changing economic and societal pattern. It furthermore seeks to find a new balance between and across generations.

www.aeip.net