PensionsEurope position paper on digital operational resilience

April 2021

www.pensionseurope.eu

1. PensionsEurope position paper on digital operational resilience

EU digital agenda welcome and needed

We welcome the efforts of the EU to increase the digital operational resilience of the financial sector and we recognise the importance of enhancing knowledge sharing and cooperation across the EU. We agree with the importance of a sound governance and risk management system to prevent and limit the impact of ICT-related incidents, disruptions, and threats.

IORPs are different from other financial institutions

We recognise that the financial sector is not homogeneous: as also the EC has correctly noted, significant differences exist between various financial entities in terms of size, business profiles and in relation to their exposure to digital risk meaning that also the consequences from cyber risks and ICT-related incidents faced by various financial entities differ greatly from one entity to another. The Recital 32 of the IORP II Directive (EU) 2016/2341 states *"IORPs are not mere financial institutions, but pension institutions with a social purpose that provide financial services."*. Furthermore, the Recital 32 concludes that IORPs *"should not be treated as purely financial service providers."*. Consequently, this premise should also be observed in the rules of ICT-related risks.

The occupational pension schemes are set up and managed jointly by social partners and additional costs are paid either by the organisers of the scheme (by increasing their pension contributions) or by the employees (with a reduction of their benefits). The IORP landscape across the EU is very heterogeneous in terms of scale, type of pension scheme, social and labour law, institutional design as well as contractual obligations. Nevertheless, **most IORPs in the EU are small in terms of size, which means that often they do not even have their own personnel, so they use sponsor resources. It is also common practice to outsource the majority of pension administration and investment services to specialised service provider and asset managers.**

The current low/negative yield environment makes small IORPs sensitive to any additional fixed costs, on top of the already existing investment, administration, governance, and communication costs. At the same time, we observe that in Member States with very large IORPs such as the Netherlands, national supervisory frameworks for ICT risks for IORPs are more extensive.

Due to all the above, we believe it is crucial that the specificities of IORPs are better reflected in the DORA requirements and that IORPs could at least 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.

According to the 1(1) of the DORA proposal, "*The regulation lays down the following uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience*". However, IORPs do not carry out 'business processes' at all. Another argument the EC uses as a rationale for the DORA proposal is the following (as stated in the Recital (9)): "*Legislative disparities and uneven national regulatory or supervisory approaches on ICT risk trigger obstacles to the single*

market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities with cross-border presence. Competition between the same type of financial entities operating in different Member States may equally be distorted." This might be an argument for many financial entities, but not for **IORPs** which **are not in competition, as they do not "sell" any products and only execute and manage an agreement that has been made by social partners. Therefore, the "competition distortion argument" does not support IORPs being part of the DORA proposal, and from a governance and risk perspective, many of its requirements are already imposed by the IORP II Directive.**

We do not see the benefits that all financial entities are covered by the same Regulation. As also the EC has highlighted, the rules on operational resilience could also be set by a plurality of EU financial services provisions, partly by the NIS Directive, and by existing or future national regimes. Regarding IORPs, in many countries, currently there are already in place clear and precise regulatory frameworks on the governance and management of ICT-related risks.

We find it important that any initiative at EU level on digital operational resilience shall consider the specific characteristics of the different types of financial entities. Notwithstanding the inherent cross-border nature of ICT risks, a one-size-fits-all approach would not succeed in its goal. **Regarding IORPs, we question whether the proposed Regulation is the appropriate way to achieve the goal of the EC.** According to the EC proposal for a Regulation, IORPs would be subject to the same provisions and obligations as vast financial conglomerates, which would not be proportionate. **A Directive would be more appropriate to consider the differences in various Member States, and thus avoiding a situation where similar (but not exactly the same) obligations exist at EU and national level, giving way to a substantial increase of operating costs (not only) for IORPs.**

In many countries, IORPs have had positive experiences with more flexible (principles-based) approach in regulating ICT risks. At the national level, the supervisor is able to tailor its supervisory activities to the way IORPs have organised their pension administration and investments. It may be the case that IORPs have outsourced all important administration processes, which entail the processing of personal data and the execution of payments to beneficiaries, to specialised service providers. Principle-based regulation allows supervisors to take into account this outsourcing relationship, test the resilience of organisations that execute the most critical processes from the perspective of the participant, while holding the IORP to account in terms of proper governance requirements.

Considering that in most of the countries the new DORA requirements would be added to the existing requirements (and that there are no initiatives to remove them), this would lead to additional administrative burden and an increase in fixed costs. Given the context of IORPs, which are mainly small or medium sized and must operate in a "lower for longer" environment, cost control is essential to ensure their business continuity.

To limit the extra costs to IORPs and strengthen the proportionality in the DORA requirements, we suggest to (i) make specific references to the IORP II Directive considering the specificities of IORPs (not for benefit, no product selling but executing an agreement of social partners, paritarian management, in most cases no pan-European activities etc.) and (ii) to distinguish those IORPs that outsource all ICT-related operational activities and to whom particularly relevant is to manage the ICT

third party risk as described in Chapter V. In general, at financial entity level the IORP II Directive requirements concerning governance and risk management of operational risk should be sufficient (see the following Articles of the IORP II Directive: 20 – responsibility of the management or supervisory body, 21 – general governance requirements, 25 – risk management, 28 – own risk assessment, and 31 -outsourcing). In countries with large IORPs we observe that supervisors have developed national supervisory frameworks that are quite close to the level of ambition of the DORA proposals, based on these IORP II provisions. Hence, supervisors are able to take a proportionate approach, which means that in case IORPs are bigger or run more important ICT processes, they enforce stricter rules.

At least micro, small and medium-sized IORPs should be excluded

A draft report of the EP ECON Committee aims to keep the scope of the DORA Regulation limited to relevant companies exposed to ICT risks, while also ensuring a risk-based approach. The draft report proposes to exclude from the scope of the Regulation (i) small and medium-sized insurance and reinsurance undertakings (as well as intermediaries), (ii) small and medium-sized audit firms and statutory auditors (in line with the Council discussion), and (iii) also partly ICT intra-group service providers.

Following the arguments in this paper, we are calling for an exemption of all the IORPs from the scope of the DORA (particularly see our amendment suggestions below on 'Article 2 - paragraph 1 - point o' and 'Article 3 - paragraph 1 - point 39'). **However, if that is not acceptable by the Council and EP, at least micro, small and medium-sized IORPs should be excluded from the scope** (particularly see the alternative amendment suggestion on 'Article 2 - paragraph 1 - point o' and amendment suggestion on 'Article 3 - paragraph 1 - point 50')**. Otherwise, the draft report of the EP ECON Committee remains very illogical when considering all the specificities of IORPs which make them different from other financial institutions and their risks stemming from reliance on ICT smaller.**

In any case, proportionality should be generally strengthened in DORA

Any measures to increase digital operational resilience shall be proportionate not only to the type, size, or financial profile of a relevant entity, but also to the risks they are exposed to and the systems and services that need to be protected and maintained. A more risk-based approach is needed, distinguishing between critical and less critical functions.

In our view the EC proposal is currently not sufficiently tailored to risks and needs of financial entities' specific characteristics in terms of their size and business profiles. We do welcome that proportionality has to some extent already been embedded in the rules on ICT risk management, digital resilience testing, reporting of major ICT-related incidents and oversight of critical ICT third-party service providers. However, the EC proposal does not provide IORPs with the same level of reassurance compared to the IORP II Directive in which the important justifications such as the above-mentioned Rec. 32 provide the basis for a pragmatic and helpful understanding of subsidiarity that considers the size, nature, scale and complexity of IORPs' activities/operations.

We therefore support the ESA's assessment as expressed in their joint letter to the EC, the EP and the Council from 9 February 2021 (Council document: 6107/1/21): *"The current DORA proposal*

excludes only micro-enterprises from the application of certain requirement and does not make any reference to sectoral legislation when defining the financial entities in scope. Given this, we would like to suggest a more comprehensive inclusion of the principle of proportionality in a more flexible way across the legal act".

In general, it is of utmost importance to preserve proportionality and follow a principle and risk-based approach in the design of rules. Through the whole Regulation, proportionality measures should in general always consider financial entities' size, nature, scale, complexity, and overall risk profile (and not only some of them). The shortcomings of the DORA proposal regarding proportionality include:

- Due to the horizontal approach, the specific characteristics of the financial entities are ignored.
- Financial entities that outsource all their operational activities seem to be required to set up an entire detailed framework in place. We believe that for those entities the DORA requirements (mainly) should be limited to managing the ICT critical or important third party risk.
- Financial entities are very heterogenous in nature across national markets as well as across Europe. IORPs manage pension provisions, with some of them managing less than € 10 million, while others manage even hundreds of billions.
- IORPs do not "sell" products, as they execute and manage an agreement made between social partners. This requires much more proportionality and a more principle-based approach. We suggest referring much more to commonly used and proven business standards like ISO or Cobit to align the requirements with good practices existing on the market.
- **Introducing proportionality by referring to microenterprises is not enough alone. An IORP, whose main goal is managing pension savings will by definition have a balance sheet that exceeds 2 million euro. The classification of small, medium or large entities should refer to the specific environment of the respective financial entity. As proportionality is of the utmost importance in this context, each type of financial entity needs its own 'sectoral' reference point. For IORPs we believe that only staff headcount should be taken into account in this context, disregarding the financial ceilings given that these amounts are not a good measure for determining the size of IORPs.**

Significant cost increase to small IORPs

We agree that it is important that all IORPs, including smaller IORPs, have a sound level of ICT protection. However, many IORPs are relatively small in scale and they are aware of the cost increase that the EC's proposal would cause. It is important to note that any raise in expenditures will come in detriment of the pension income of members and beneficiaries thus leading to a decline in the adequacy of their pensions, contradicting the general objective of the EU policy to strengthen consumer protection.

As proportionality for small and medium sized IORPs is completely lacking in the proposal and the required measures all come with a fixed cost, we fear that mainly small and medium sized IORPs, and thus their members and beneficiaries, will be highly negatively impacted by these measures. Any extra measures should only be considered after performing a thorough cost/benefit-analysis and should only be implemented if they really represent an added value. Finally, it should be noted that apart from the

above-mentioned cost-increase linked to these additional measures, this Regulation will also bring about additional costs for the supervisory authorities which in turn will be passed on to the financial entities under their supervision.

High number of empowerments to the EC to adopt TRSs

Finally, we are concerned about the disconcertingly high number of empowerments to the EC to adopt technical regulatory standards (TRSs) and very detailed requirements on key contractual provisions for arrangements with ICT third-party service providers. For IORPs this regulatory instrument is not suitable regarding the IORP II Directive's approach of a "minimum harmonisation" (Recital 3 of the IORP II Directive). Recent experiences with empowerments for TRS in European regulation have given reason for even more concern. Especially in the ESA's drafts (the latest examples are the draft-RTS on sustainability-related disclosures in the financial services sectors) **we have observed a tendency to exceed the scope of the level-l-authorisation and to not adequately consider (or to even ignore) existing provisions on proportionality in the text of the regulation.** We therefore would like to reiterate the idea of addressing these issues in a Directive to give the Member States the required latitude in the transposition process.

Request for more a stringent, less redundant regulation

On a general note, PensionsEurope recommends an editorial revision of the entire proposal with the overarching goal to reduce redundancies and the overall level of detail in favour of a more principle-based approach. In many instances, we feel that existing regulation for IORPs at the national level already considers the purpose (ratio legis) of many of the proposed provisions. But even in these cases, the very prescriptive and details-oriented wording of the Regulation's provision could entail procedural changes and increase the efforts and especially the costs for documenting full compliance.

Reconsider the requirements on incident reporting

The NIS Directive introduced incident reporting for the financial entities within its scope. These entities have to report with their national cybersecurity centre, which in return provides support, information and advice. Pension funds do not fall within the scope of this requirement. The requirements of the DORA proposal to report material incidents within hours therefore is a significant extension of the framework, also in countries with larger IORPs.

The requirement seems disproportionate for two reasons. First, it would mean that in the midst of a breach, staff would be required to spend time and resource on incident reporting, rather than mitigating the impact of the breach itself. Second, the reporting requirement does not seem to be linked to a commitment for support, information or advice by national cybersecurity centres, as currently is the case with entities falling within scope of the NIS Directive. Therefore, the effort that is being spent on reporting will not in fact help the IORP with tackling the crisis but will only be undertaking for compliance purposes.

PensionsEurope therefore urges a reconsideration of the usefulness and impact of the incident reporting requirements. In case an incident reporting requirement would be maintained for entities

that fall outside the scope of the NIS Directive, the burden could be reduced by raising the materiality threshold and extending the deadlines.

Amendment suggestions on the EC proposal

Title:

Text proposed by the Commission	*Amendment*
Proposal for a ***REGULATION*** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 […] HAVE ADOPTED THIS ***REGULATION***:	Proposal for a ***DIRECTIVE*** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 […] HAVE ADOPTED THIS ***DIRECTIVE***:

General remarks on the Recitals

The following amendment proposals to the Recitals cannot claim to be exhaustive. Apart from the semantic aspect of all mentions to a "Regulation" having to be replaced by "Directive", we do not share the EC's premise that is imperative to subject all financial entities to essentially the same set of rules. Accordingly, numerous other Recitals would have to be thoroughly reworked following our recommendation to give more attention to the principle of proportionality and to adequately respect the differences that exist between various financial entities in terms of size, business profiles and in relation to their exposure to digital risks.

Recital 5:

Text proposed by the Commission	*Amendment*
Despite national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and stability of the Union financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed at safeguarding the Union's competitiveness and stability from economic, prudential and market conduct perspectives. ***Though ICT security and digital resilience are part of operational risk, they have been less in the focus of the post-crisis regulatory agenda, and have only developed in some areas of the***	Despite national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and stability of the Union financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed at safeguarding the Union's competitiveness and stability from economic, prudential and market conduct perspectives. ***Whilst contributing to strengthening and harmonising ICT security and digital resilience at the EU level, this Directive will also properly take into account already existing regulatory***

Union's financial services policy and regulatory landscape, or only in a few Member States.	***standards, avoid unnecessary redundancies, asynchronous requirements and provide enough flexibility for complying with the requirements of this Directive.***

Recital 10 - paragraph 1:

Text proposed by the Commission	*Amendment*
The partial way in which the ICT-risk related provisions have until now been addressed at Union level shows gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and creates inconsistencies due to emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user like ***finance since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union***.	The partial way in which the ICT-risk related provisions have until now been addressed at Union level shows gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and creates ***in case of cross-border financial entities*** inconsistencies due to emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user like ***some cross-border financial entities.***

Recital 10 - paragraph 2 (new):

Text proposed by the Commission	*Amendment*
	Consequently, the Directive pursues the harmonisation of the already existing national frameworks and the closing of regulatory gaps to prevent problems especially for cross-border financial entities. At the same time, the Directive acknowledges the efforts made so far at Member State level.

Recital 14:

Text proposed by the Commission	*Amendment*
(14) The use of a regulation helps reducing regulatory complexity, fosters supervisory convergence, increases legal certainty, while	***deleted***

also contributing to limiting compliance costs, especially for financial entities operating cross-border, and to reducing competitive distortions. The choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities appears therefore the most appropriate way to guarantee a homogenous and coherent application of all components of the ICT risk management by the Union financial sectors.	

Recital 14 (new):

Text proposed by the Commission	*Amendment*
	Notwithstanding the high degree of interconnection between financial services, differences between different types of financial entities regarding their risk exposure and risk profiles remain. Stipulating fully uniform requirements at the EU level by means of a regulation would therefore be neither necessary nor proportionate. The use of a Directive can make a significant contribution to harmonising the regulatory frameworks in the Member States and to close remaining regulatory gaps while at the same time giving Member States leeway for making necessary adjustments for specific types of financial entities in the transposition process.

Recital 20:

Text proposed by the Commission	*Amendment*
(20) To remain in full control of ICT risks, financial entities need to have in place ***comprehensive*** capabilities enabling a strong and effective ICT risk management, alongside specific mechanisms and policies for ICT-related incident reporting, testing of ICT systems,	(20) To remain in full control of ICT risks, financial entities need to have in place ***appropriate*** capabilities enabling a strong and effective ICT risk management, alongside specific mechanisms and policies for ICT-related incident reporting, testing of ICT systems,

controls and processes, as well as for managing ICT third-party risk. The digital operational resilience bar for the financial system should be raised while allowing for a proportionate application of requirements ***for financial entities which are micro enterprises as defined in Commission Recommendation 2003/361/EC.***	controls and processes, as well as for managing ICT third-party risk. The digital operational resilience bar for the financial system should be raised while allowing for a proportionate application of requirements ***whilst taking into account the size, nature, scale and complexity of the risks inherent in the activities of the institutions and the ICT-risks resulting therefrom. At the same time, the application of requirements follows the principle of materiality: only significant risks have to be considered.***

Recital 33:

Text proposed by the Commission	*Amendment*
(33) Notwithstanding the broad coverage envisaged by this ***Regulation***, the application of the digital operational resilience rules should take into consideration significant differences between financial entities in terms of size, business profiles or exposure to digital risk. As a general principle, when directing resources and capabilities to the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size ***and business profile***, while competent authorities should continue to assess and review the approach of such distribution.	(33) Notwithstanding the broad coverage envisaged by this ***Directive***, the application of the digital operational resilience rules should take into consideration significant differences between financial entities in terms of size, business profiles or exposure to digital risk. As a general principle, when directing resources and capabilities to the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size, ***nature, scale and complexity of the risks inherent to their activities and the ICT risks resulting therefrom,*** while competent authorities should continue to assess and review the approach of such distribution.

Recital 34 - paragraph 1:

Text proposed by the Commission	*Amendment*
(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities which are not micro enterprises in the	(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities which are not micro, ***small, or medium-***

sense of this ***Regulation*** should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, or to adopt a human resources document comprehensively explaining access rights policies.	***sized*** enterprises in the sense of this ***Directive or where the application of this requirement does not contradict the proportionality principle*** should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, or to adopt a human resources document comprehensively explaining access rights policies.

Recital 35:

Text proposed by the Commission	*Amendment*
(35) Moreover, as solely those financial entities identified as significant for the purposes of the advanced digital resilience testing should be required to conduct threat led penetration tests, the administrative processes and financial costs entailed by the performance of such tests should be devolved to a small percentage of financial entities. Finally, with a view to ease regulatory burdens, only financial entities other than micro enterprises should be asked to regularly report to the competent authorities all costs and losses caused by ICT disruptions and the results of post-incident reviews after significant ICT disruptions.	(35) Moreover, as solely those financial entities identified as significant for the purposes of the advanced digital resilience testing should be required to conduct threat led penetration tests, the administrative processes and financial costs entailed by the performance of such tests should be devolved to a small percentage of financial entities. Finally, with a view to ease regulatory burdens, only financial entities other than micro***, small and medium-sized*** enterprises should be asked to regularly report to the competent authorities all costs and losses caused by ***significant*** ICT disruptions and the results of post-incident reviews after significant ICT disruptions.

Recital 64:

Text proposed by the Commission	*Amendment*
(64) The Oversight Framework shall not replace, or in any way nor for any part substitute the management by financial entities	(64) The Oversight Framework shall not replace, or in any way nor for any part substitute the management by financial entities

of the risk entailed by the use of ICT third-party service providers, including the obligation of ongoing monitoring of their contractual arrangements concluded with critical ICT third-party service providers, and shall not affect the full responsibility of the financial entities in complying with, and discharging of, all requirements under this Regulation and relevant financial services legislation. ***To avoid duplications and overlaps, competent authorities should refrain from individually taking any measures aimed at monitoring the critical ICT third-party service provider's risks Any such measures should be previously coordinated and agreed in in the context of the Oversight Framework.***	of the risk entailed by the use of ICT third-party service providers, including the obligation of ongoing monitoring of their contractual arrangements concluded with critical ICT third-party service providers, and shall not affect the full responsibility of the financial entities in complying with, and discharging of, all requirements under this Regulation and relevant financial services legislation.

Recital 73:

Text proposed by the Commission	*Amendment*
(73) Since the objectives of this Regulation, namely to achieve a high level of digital operational resilience applicable to all financial entities, cannot be sufficiently achieved by the Member States because they require the harmonisation of a multitude of different rules, currently existing either in some Union acts, either in the legal systems of the various Member States, but can rather, because of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	***deleted***

General remarks on all the Articles

In accordance with our recommendation to transform the DORA proposal from a Regulation to a Directive, most Articles require a major overhaul in terms of wording and phrasing to reflect the fundamental differences in the legal nature of Directives and Regulations.

Apart from formal aspects like the use of conventional introductory expressions such as "The Member States shall ensure …", the prescriptive nature and the level of detail in many Articles should be reduced appropriately. Nevertheless, most of the suggested amendments are considered necessary irrespective of whether the proposal will remain a Regulation or whether it will be transformed to a Directive.

CHAPTER I – GENERAL PROVISIONS

Following the arguments in this paper, we are calling for an exemption of all the IORPs from the scope of the DORA:

Personal scope
Article 2 - paragraph 1 - point o:

Text proposed by the Commission	*Amendment*
(o) institutions for occupational retirement pensions,	***deleted***

Definitions
Article 3 - paragraph 1 - point 39:

Text proposed by the Commission	*Amendment*
(39) 'institution for occupational retirement pensions' means institution for occupational retirement pensions as defined in point (6) of Article 1 of Directive 2016/2341;	***deleted***

However, if the Council and the EP finally conclude that the largest IORPs should be included in the scope of the DORA, it should be made clear that micro, small and medium-sized IORPs are excluded (otherwise, the draft report of the EP ECON Committee remains very illogical when considering all the specificities of IORPs which make them different from other financial institutions and their risks stemming from reliance on ICT smaller). Please find below our alternative amendment suggestions:

An alternative amendment suggestion (together with the below clarifying amendment to 'Article 3 - paragraph 1 - point 50'):

Article 2 - paragraph 1 - point o:

Text proposed by the Commission	*Amendment*
(o) institutions for occupational retirement pensions,	(o) institutions for occupational retirement pensions, ***unless they are micro, small or medium-sized enterprises,***

An alternative amendment suggestion clarifying the above alternative amendment to 'Article 2 - paragraph 1 - point o' (partly aligned with the EP ECON draft report proposal):

Article 3 - paragraph 1 - point 50:

Text proposed by the Commission	*Amendment*
(50) '***microenterprise***' means a financial entity as defined in Article ***2(3)*** of the Annex to Recommendation 2003/361/EC.	(50) '***micro, small and medium-sized enterprise***' means a financial entity as defined in Article ***2*** of the Annex to Recommendation 2003/361/EC. ***Given the specific nature of institutions for occupational retirement provisions, only the criterium of the number of employees is applied for them.***

CHAPTER II – ICT RISK MANAGEMENT

Governance and organisation

Article 4 - paragraph 2:

Text proposed by the Commission	*Amendment*
The management body of the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework ***referred to in Article 5(1)***: For the purposes of the first subparagraph, the management body shall: (a) bear the final responsibility for managing the financial entity's ICT risks;	The management body of the financial entity***, with due consideration to its size, nature, scale, complexity, and risk profile,*** shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework ***thus bearing the final responsibility for managing the entity's ICT risks***: For the purposes of the first subparagraph, ***a distinction is made between financial entities***

(b) set clear roles and responsibilities for all ICT-related functions; (c) determine the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in point (b) of Article 5(9); (d) approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan referred to in, respectively, paragraphs 1 and 3 of Article 10; (e) approve and periodically review the ICT audit plans, ICT audits and material modifications thereto; (***f***) allocate and periodically review appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including training on ICT risks and skills for all relevant staff; ***(g) approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;*** ***(h) be duly informed, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes;*** ***(i) be duly informed about ICT-related incidents and their impact and about response, recovery and corrective measures.***	***that outsource all ICT services to run their business operations on the one hand and financial entities that do not on the other hand.*** ***T***he management body ***of financial entities that outsource all ICT services to run their business operations*** shall: (a) bear the final responsibility for managing the financial entity's ICT risks; ***(b) approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;*** ***(c) be duly informed, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes;*** ***(d) be duly informed about ICT-related incidents and their impact and about response, recovery and corrective measures.*** ***The management body of financial entities that outsource all ICT services to run their business operations shall define a holistic ICT multi-vendor strategy at entity level showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of third-party service providers.*** ***The management body of financial entities other than those that outsource all ICT services to run their business operations shall on top:*** (b) set clear roles and responsibilities for all ICT-related functions;

	(c) determine the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in point (b) of Article 5(9); (d) approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan referred to in, respectively, paragraphs 1 and 3 of Article 10; (e) approve and periodically review the ICT audit plans, ICT audits and material modifications thereto; (***e***) allocate and periodically review appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including training on ICT risks and skills for all relevant staff;

Article 4 - paragraph 4:

Text proposed by the Commission	*Amendment*
Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity.	Members of the management body ***of financial entities other than those that outsource all ICT services to run their business operations*** shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity.

Article 4 - paragraph 4 (new):

Text proposed by the Commission	*Amendment*
	Financial entities as referred to in Article 3 (39) shall put in place the requirements as referred to in paragraph 1 in accordance with the articles 20, 21, 25 and 28 of Directive (EU) 2016/2341.

ICT risk management framework

Article 5 - paragraph 1:

Text proposed by the Commission	*Amendment*
Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience that matches their ***business needs,*** size ***and complexity***.	Financial entities shall have ***as an integral part of their overall risk management systems*** a sound, comprehensive and well-documented ICT risk management framework, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience that matches their size***, nature, scale and complexity of the risks inherent to their activities and the ICT risks resulting therefrom.***

Article 5 - paragraph 6:

Text proposed by the Commission	*Amendment*
The ICT risk management framework referred to in paragraph 1 shall be documented and reviewed ***at least once a year***, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring.	The ICT risk management framework referred to in paragraph 1 shall be documented and reviewed ***on a regular basis***, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring.

Article 5 - paragraph 7:

Text proposed by the Commission	*Amendment*
The ICT risk management framework referred to in paragraph 1 shall be audited on a regular basis by ICT auditors possessing sufficient knowledge, skills and expertise in ICT risk. The frequency and focus of ICT audits shall be commensurate to the ICT risks of the financial entity.	***deleted***

Article 5 - paragraph 8:

Text proposed by the Commission	*Amendment*
A formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings, shall be established, taking into consideration the conclusions from the audit review while having due regard to the nature, scale and complexity of the financial entities' services and activities.	***deleted***

Article 5 - paragraph 9:

Text proposed by the Commission	*Amendment*
The ICT risk management framework referred to in paragraph 1 shall include a digital resilience strategy setting out how the framework is implemented. To that effect it shall include the methods to address ICT risk and attain specific ICT objectives, by:	The ICT risk management framework referred to in paragraph 1 shall ***for financial entities other than micro, small and medium-sized enterprises*** include a digital resilience strategy setting out how the framework is implemented. To that effect it shall include the methods to address ICT risk and attain specific ICT objectives, by:

Article 5 - paragraph 9 - point f:

Text proposed by the Commission	*Amendment*
(f) ***evidencing the number of reported major ICT-related incidents and*** the effectiveness of preventive measures	(f) the effectiveness of preventive measures

Article 5 - paragraph 9 - point g:

Text proposed by the Commission	*Amendment*
(g) defining a holistic ICT multi-vendor strategy at entity level showing key dependencies on ICT third-party service providers and	***deleted***

explaining the rationale behind the procurement mix of third-party service providers	

Article 5 - paragraph 10 (new):

Text proposed by the Commission	*Amendment*
	After notification of competent authorities, financial entities that outsource all ICT services to run their business operations may delegate the tasks as set out in the Articles 6 through 14 to intra-group or external undertakings (such as the ICT third-party service provider(s) to whom the ICT services are outsourced to). The management body of the financial entity shall however – in accordance with Article 4.2.(a) - bear the final responsibility for managing the financial entity's ICT risks.

Identification

Article 7 - paragraph 1:

Text proposed by the Commission	*Amendment*
As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial entities shall review as needed***, and at least yearly,*** the adequacy of the classification of the information assets and of any relevant documentation.	As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial entities shall review as needed the adequacy of the classification of the information assets and of any relevant documentation.

Article 7 - paragraph 2:

Text proposed by the Commission	*Amendment*

Financial entities shall on a continuous basis identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT-related business functions and information assets. Financial entities shall review on a regular basis***, and at least yearly,*** the risk scenarios impacting them.	Financial entities ***other than micro, small and medium-sized enterprises*** shall on a continuous basis identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT-related business functions and information assets. Financial entities shall review on a regular basis the risk scenarios impacting them.

Article 7 paragraph 3:

Text proposed by the Commission	*Amendment*
Financial entities other than ***microenterprises*** shall on a regular basis***, and at least yearly,*** conduct a specific ICT risk assessment on all legacy ICT systems, especially before and after connecting old and new technologies, applications or systems.	Financial entities other than ***micro, small and medium-sized enterprises*** shall on a regular basis conduct a specific ***and appropriate*** ICT risk assessment on all ***critical*** legacy ICT systems, especially before and after connecting old and new technologies, applications or systems.

Article 7 - paragraph 6:

Text proposed by the Commission	*Amendment*
For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain and regularly update relevant inventories.	For the purposes of paragraphs 1, 4 and 5, financial entities ***other than micro, small and medium-sized enterprises*** shall maintain and regularly update relevant inventories.

Protection and Prevention

Article 8 - paragraph 1:

Text proposed by the Commission	*Amendment*
For the purposes of adequately protecting the ICT systems and with a view to organising response measures, financial entities shall ***continuously*** monitor and control the functioning of the ICT systems and tools and shall minimise the impact of such risks through	For the purposes of adequately protecting the ICT systems and with a view to organising response measures, financial entities shall monitor and control the functioning of the ICT systems and tools and shall minimise the impact of such risks through the deployment of

the deployment of appropriate ICT security tools, policies and procedures.	appropriate ICT security tools, policies and procedures.

Article 8 - paragraph 4:

Text proposed by the Commission	*Amendment*
As part of the ICT risk management framework referred to in Article 5(1), financial entities shall: (a) develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of theirs, and their customers' ICT resources, data and information assets; (b) following a risk-based approach, establish a sound network and infrastructure management using appropriate techniques, methods and protocols including implementing automated mechanisms to isolate affected information assets in case of cyber-attacks; (c) implement policies that limit the physical and virtual access to ICT system resources and data to what is required only for legitimate and approved functions and activities, and establish to that effect a set of policies, procedures and controls that address access privileges and a sound administration thereof; (d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access to cryptographic keys whereby data is encrypted based on results of approved data classification and risk assessment processes; (e) implement policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, system or security changes, that are based on a risk-assessment approach and as an integral part of the financial entity's overall change management process, in order	***Deleted (or to be merged with Article 5 in order to avoid duplications/redundancies)***

to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner; (f) have appropriate and comprehensive policies for patches and updates. For the purposes of point (b), financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed and shall ensure its compartmentalisation and segmentation, in order to minimise and prevent contagion, especially for interconnected financial processes. For the purposes of point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.	

Detection

Article 9 - paragraph 1:

Text proposed by the Commission	*Amendment*
Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, including ICT network performance issues and ICT-related incidents, and to identify all potential material single points of failure. All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 22.	Financial entities shall***, with due consideration to their size, nature, scale, complexity, and risk profiles,*** have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, including ICT network performance issues and ICT-related incidents, and to identify all potential material single points of failure. All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 22.

Article 9 - paragraph 2:

Text proposed by the Commission	*Amendment*

The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger ICT-related incident detection and ICT-related incident response processes, and shall put in place automatic alert mechanisms for relevant staff in charge of ICT-related incident response.	The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger ICT-related incident detection and ICT-related incident response processes, and shall ***for financial entities other than micro, small and medium-sized enterprises*** put in place automatic alert mechanisms for relevant staff in charge of ICT-related incident response.

Article 9 - paragraph 3:

Text proposed by the Commission	*Amendment*
Financial entities shall devote sufficient resources and capabilities, with due consideration to their size, ***business*** and risk profiles, to monitor ***user activity,*** occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.	Financial entities ***other than micro, small and medium-sized enterprises*** shall devote sufficient resources and capabilities, with due consideration to their size, ***nature, scale, complexity*** and risk profiles, to monitor occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.

Response and recovery

Article 10 - paragraph 1:

Text proposed by the Commission	*Amendment*
As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial entities shall put in place a dedicated and comprehensive ICT Business Continuity Policy as an integral part of the operational business continuity policy of the financial entity.	As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial entities shall put in place a dedicated and comprehensive ICT Business Continuity Policy as an integral part of the operational business continuity policy of the financial entity. ***This ICT Business Continuity Policy is aligned with common practices and recognised international standards.***

Article 10 - paragraph 2:

Text proposed by the Commission	*Amendment*

Financial entities shall implement the ICT Business Continuity Policy referred to in paragraph 1 through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at: ***(a) recording all ICT-related incidents;*** ***(b) ensuring the continuity of the financial entity's critical functions;*** ***(c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in particular but not limited to cyber-attacks, in a way which limits damage and prioritises resumption of activities and recovery actions;*** ***(d) activating without delay dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and preventing further damage, as well as tailored response and recovery procedures established in accordance with Article 11;*** ***(e) estimating preliminary impacts, damages and losses;*** ***(f) setting out communication and crisis management actions which ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 13, and reported to competent authorities in accordance with Article 17.***	***deleted***

Article 10 - paragraph 4:

Text proposed by the Commission	*Amendment*
Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.	Financial entities ***other than micro, small and medium-sized enterprises*** shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.

Article 10 - paragraph 5 - point a:

Text proposed by the Commission	*Amendment*
(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan ***at least yearly*** and after substantive changes to the ICT systems;	(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan ***on a regular basis*** and after substantive changes to the ICT systems;

Article 10 – paragraph 6:

Text proposed by the Commission	*Amendment*
Financial entities other than ***microenterprises*** shall have a crisis management function, which, in case of activation of their ICT Business Continuity Policy or ICT Disaster Recovery Plan, shall set out clear procedures to manage internal and external crisis communications in accordance with Article 13.	Financial entities other than ***micro, small and medium-sized enterprises*** shall have a crisis management function, which, in case of activation of their ICT Business Continuity Policy or ICT Disaster Recovery Plan, shall set out clear procedures to manage internal and external crisis communications in accordance with Article 13.

Article 10 – paragraph 9:

Text proposed by the Commission	*Amendment*
*Financial entities other than **microenterprises** shall report to competent authorities **all** costs and losses caused by ICT disruptions and ICT-related incidents.*	*Financial entities other than **micro, small and medium-sized enterprises** shall report to competent authorities costs and losses caused by **significant** ICT disruptions and ICT-related incidents.*

Backup policies and recovery methods
Article 11 - paragraph 1:

Text proposed by the Commission	*Amendment*
For the purpose of ensuring the restoration of ICT systems with minimum downtime and	For the purpose of ensuring the restoration of ICT systems with minimum downtime and

limited disruption, as part of their ICT risk management framework, financial entities shall develop: (a) a backup policy specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the sensitiveness of the data; (b) recovery methods.	limited disruption, as part of their ICT risk management framework, financial entities shall develop: (a) a backup policy specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the sensitiveness of the data; (b) recovery methods. ***These ICT backup and recovery methods are aligned with common practices and recognised international standards with due consideration to the size, nature, scale and complexity of financial institutions' activities.***

Article 11 - paragraph 4:

Text proposed by the Commission	*Amendment*
Financial entities shall maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.	Financial entities ***other than micro, small and medium-sized enterprises*** shall maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.

Article 11 - paragraph 6:

Text proposed by the Commission	*Amendment*
In determining the recovery time and point objectives for each function, financial entities shall take into account the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.	In determining the recovery time and point objectives for each ***essential*** function, financial entities shall take into account the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.

Article 11 - paragraph 7:

Text proposed by the Commission	*Amendment*

When recovering from ***an*** ICT-related incident, financial entities shall perform ***multiple*** checks, including reconciliations, in order to ensure that the level of data integrity is of the highest level. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.	When recovering from ***a critical*** ICT-related incident, financial entities shall perform checks, including reconciliations, in order to ensure that the level of data integrity is of the highest level. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

Learning and evolving

Article 12 - paragraph 1:

Text proposed by the Commission	*Amendment*
Financial entities shall have in place capabilities and staff, suited to their size, ***business*** and risk profiles, to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse their likely impacts on their digital operational resilience.	Financial entities shall have in place capabilities and staff, suited to their size, ***nature, scale and complexity of their activities*** and risk profiles ***resulting therefrom,*** to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse their likely impacts on their digital operational resilience.

Article 12 - paragraph 2 - subparagraph 2:

Text proposed by the Commission	*Amendment*
When implementing changes, financial entities other than microenterprises shall communicate those changes to the competent authorities.	***deleted***

Article 12 - paragraph 2 - subparagraph 3:

Text proposed by the Commission	*Amendment*
The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to:	***deleted***

(a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity; ***(b) the quality and speed in performing forensic analysis;*** ***(c) the effectiveness of incident escalation within the financial entity;*** ***(d) the effectiveness of internal and external communication.***	

Article 12 - paragraph 4:

Text proposed by the Commission	*Amendment*
Financial entities shall monitor the effectiveness of the implementation of their digital resilience strategy set out in Article 5(9). They shall map the evolution of ICT risks over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understand the level of ICT risk exposure and enhance the cyber maturity and preparedness of the financial entity.	Financial entities ***other than micro, small and medium-sized enterprises*** shall monitor the effectiveness of the implementation of their digital resilience strategy set out in Article 5(9). They shall map the evolution of ICT risks over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understand the level of ICT risk exposure and enhance the cyber maturity and preparedness of the financial entity.

Article 12 - paragraph 5:

Text proposed by the Commission	*Amendment*
Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.	Senior ICT staff shall report at least yearly to the management body ***of financial entities other than micro, small and medium-sized enterprises*** on the findings referred to in paragraph 3 and put forward recommendations.

Article 12 - paragraph 6 - subparagraph 1:

Text proposed by the Commission	*Amendment*

Financial entities shall ***develop ICT security*** awareness ***programs and digital operational resilience trainings as compulsory modules in their staff training schemes. These shall be applicable to all employees and to senior management staff.***	Financial entities shall ***raise*** awareness ***among their employees and governing and managing bodies of the importance of digital operational resilience.***

Article 12 - paragraph 6 - subparagraph 2:

Text proposed by the Commission	*Amendment*
Financial entities shall monitor relevant technological developments on a continuous basis, also with a view to understand possible impacts of deployment of such new technologies upon the ICT security requirements and digital operational resilience. They shall keep abreast of the latest ICT risk management processes, effectively countering current or new forms of cyber-attacks.	Financial entities***, with due consideration to their size, nature, scale, complexity, and risk profiles,*** shall monitor relevant technological developments on a continuous basis, also with a view to understand possible impacts of deployment of such new technologies upon the ICT security requirements and digital operational resilience. They shall keep abreast of the latest ICT risk management processes, effectively countering current or new forms of cyber-attacks.

Communication

Article 13 - paragraph 1:

Text proposed by the Commission	*Amendment*
As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place communication plans enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate.	As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place communication plans***, suited to their size, nature, scale and complexity of their activities and the risk profiles resulting therefrom, thus*** enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate.

Article 13 - paragraph 2:

Text proposed by the Commission	*Amendment*

As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement communication policies for staff and for external stakeholders. ***Communication policies for staff shall take into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.***	As part of the ICT risk management framework referred to in Article 5(1), financial entities ***other than micro, small and medium-sized enterprises*** shall implement communication policies for staff and for external stakeholders.

Article 13 - paragraph 2:

Text proposed by the Commission	*Amendment*
As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement communication policies for staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.	As part of the ICT risk management framework referred to in Article 5(1), financial entities ***other than micro, small and medium-sized enterprises*** shall implement communication policies for staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.

Article 13 - paragraph 3:

Text proposed by the Commission	*Amendment*
At least one person in the entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the role of public and media spokesperson for that purpose	***In financial entities other than micro, small and medium-sized enterprises, at*** least one person in the entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the role of public and media spokesperson for that purpose.

Further harmonisation of ICT risk management tools, methods, processes and policies

Article 14:

Text proposed by the Commission	*Amendment*

The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) shall, in consultation with the European Union Agency on Cybersecurity (ENISA), develop draft regulatory technical standards for the following purposes: ***(a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 8(2), with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the authenticity and integrity of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions;*** ***(b) prescribe how the ICT security policies, procedures and tools referred to in Article 8(2) shall incorporate security controls into systems from inception (security by design), allow for adjustments to the evolving threat landscape, and provide for the use of defence-in-depth technology;*** ***(c) specify further the appropriate techniques, methods and protocols referred to in point (b) of Article 8(4);*** ***(d) develop further components of the controls of access management rights referred to in point (c) of Article 8(4) and associated human resources policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risks through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;*** ***(e) develop further the elements specified in Article 9(1) enabling a prompt detection of anomalous activities and the criteria referred to in Article 9(2) triggering ICT-related incident detection and response processes;***	***deleted***

(f) specify further the components of the ICT Business Continuity Policy referred to in Article 10(1); ***(g) specify further the testing of ICT business continuity plans referred to in Article 10(5) to ensure that it duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency or other failures of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;*** ***(h) specify further the components of the ICT Disaster Recovery Plan referred to in Article 10(3).*** ***EBA, ESMA and EIOPA shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 1 year after the date of entry into force].*** ***Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.***	

CHAPTER III - ICT-RELATED INCIDENTS - MANAGEMENT, CLASSIFICATION AND REPORTING

ICT-related incident management process

Article 15 - paragraph 1:

Text proposed by the Commission	*Amendment*
Financial entities shall establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents ***and shall put in place early warning indicators as alerts***.	Financial entities shall establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.

Article 15 - paragraph 3:

Text proposed by the Commission	*Amendment*
The ICT-related incident management process ***referred to in paragraph 1*** shall***:*** ***(a) establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and to the severity and criticality of the services impacted, in accordance with the criteria referred to in Article 16(1);*** ***(b) assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;*** ***(c) set out plans for communication to staff, external stakeholders and media in accordance with Article 13, and for notification to clients, internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;*** ***(d) ensure that major ICT-related incidents are reported to relevant senior management and inform the management body on major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of ICT-related incidents;*** ***(e) establish ICT-related incident response procedures to mitigate impacts and ensure that services becomes operational and secure in a timely manner.***	The ICT-related incident management process shall ***be in line with good practices and recognised international standards.***

Article 15 - paragraph 3 (new):

Text proposed by the Commission	*Amendment*
	After notification of competent authorities, financial entities that outsource all ICT services to run their business operations may delegate the tasks as set out in the Articles 15 through 20 to intra-group or external undertakings

	(such as the ICT third-party service provider(s) to whom the ICT services are outsourced to). The management body of the financial entity shall however – in accordance with Article 4.2.(a) - bear the final responsibility for managing the financial entity's ICT risks.

Classification of ICT-related incidents

Article 16:

Text proposed by the Commission	*Amendment*
1. Financial entities shall classify ICT-related incidents ***and shall determine their impact based on the following criteria:*** ***(a) the number of users or financial counterparts affected by the disruption caused by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;*** ***(b) the duration of the ICT-related incident, including service downtime;*** ***(c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;*** ***(d) the data losses that the ICT-related incident entails, such as integrity loss, confidentiality loss or availability loss;*** ***(e) the severity of the impact of the ICT-related incident on the financial entity's ICT systems;*** ***(f) the criticality of the services affected, including the financial entity's transactions and operations;*** ***(g) the economic impact of the ICT-related incident in both absolute and relative terms.*** ***2. The ESAs shall, through the Joint Committee of the ESAs (the 'Joint Committee') and after consultation with the European Central Bank (ECB) and ENISA, develop common draft regulatory technical standards further specifying the following:***	1. Financial entities shall classify ICT-related incidents ***in line with good practices and recognised international standards.***

(a) the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents which are subject to the reporting obligation laid down in Article 17(1); ***(b) the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents to other Member States' jurisdictions, and the details of ICT-related incidents reports to be shared with other competent authorities pursuant to points (5) and (6) of Article 17.*** ***3. When developing the common draft regulatory technical standards referred to in paragraph 2, the ESAs shall take into account international standards, as well as specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors.*** ***The ESAs shall submit those common draft regulatory technical standards to the Commission by [PO: insert date 1 year after the date of entry into force].*** ***Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 2 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.***	

Reporting of major ICT-related incidents
Article 17 - paragraph 1 - subparagraph 2:

Text proposed by the Commission	*Amendment*
For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, an incident report ***using the template referred to in Article 18*** and submit it to the competent authority.	For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, an incident report and submit it to the competent authority.

Article 17 - paragraph 1 - subparagraph 3:

Text proposed by the Commission	*Amendment*
The report shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.	The report shall include all ***relevant*** information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.

Article 17 - paragraph 3 - point a:

Text proposed by the Commission	*Amendment*
(a) an initial notification, without delay, ***but no later than the end of the business day, or, in case of a major ICT-related incident that took place later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day, or,*** where reporting channels are not available, as soon as they become available;	*(a) an initial notification, without delay, where reporting channels are not available, as soon as they become available*;

Harmonisation of reporting content and templates
Article 18:

Text proposed by the Commission	*Amendment*
The ESAs, through the Joint Committee and after consultation with ENISA and the ECB, shall develop: ***(a) common draft regulatory technical standards in order to:*** ***(1) establish the content of the reporting for major ICT-related incidents;*** ***(2) specify further the conditions under which financial entities may delegate to a third-party service provider, upon prior approval by the***	***deleted***

competent authority, the reporting obligations set out in this Chapter; ***(b) common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident. The ESAs shall submit the common draft regulatory technical standards referred to in point (a) of paragraph 1 and the common draft implementing technical standards referred to in point (b) of the paragraph 1 to the Commission by xx 202x [PO: insert date 1 year after the date of entry into force].*** ***Power is delegated to the Commission to supplement this Regulation by adopting the common regulatory technical standards referred to in point (a) of paragraph 1 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.*** ***Power is conferred on the Commission to adopt the common implementing technical standards referred to in point (b) of paragraph 1 in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.***	

Centralisation of reporting of major ICT-related incidents
Article 19:

Text proposed by the Commission	*Amendment*
1. The ESAs, through the Joint Committee and in consultation with ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The report shall explore	***deleted***

ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence. ***2. The report referred to in the paragraph 1 shall comprise at least the following elements:*** ***(a) prerequisites for the establishment of such an EU Hub;*** ***(b) benefits, limitations and possible risks;*** ***(c) elements of operational management;*** ***(d) conditions of membership;*** ***(e) modalities for financial entities and national competent authorities to access the EU Hub;*** ***(f) a preliminary assessment of financial costs entailed by the setting-up the operational platform supporting the EU Hub, including the required expertise*** ***3. The ESAs shall submit the report referred to in the paragraph 1 to the Commission, the European Parliament and to the Council by xx 202x [OJ: insert date 3 years after the date of entry into force].***	

CHAPTER IV - DIGITAL OPERATIONAL RESILIENCE TESTING

General requirements for the performance of digital operational resilience testing
Article 21 - paragraph 1:

Text proposed by the Commission	*Amendment*
For the purpose of assessing preparedness for ICT-related incidents, of identifying weaknesses, deficiencies or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities shall establish, maintain and review, with due consideration to their size, business and risk profiles, a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk	For the purpose of assessing preparedness for ICT-related incidents, of identifying weaknesses, deficiencies or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities shall establish, maintain and review, with due consideration to their size, business and risk profiles, ***nature, scale and complexity of the risks inherent to their activities and the ICT risks resulting therefrom***, a sound and

management framework referred to in Article 5.	comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework referred to in Article 5.

Article 21 - paragraph 2:

Text proposed by the Commission	*Amendment*
The digital operational resilience testing ***programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with the provisions of Articles 22 and 23.***	The digital operational resilience testing shall ***be in line with good practices and recognised international standards.***

Article 21 - paragraph 3:

Text proposed by the Commission	*Amendment*
Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing programme referred to in paragraph 1, taking into account the evolving landscape of ICT risks, any specific risks to which the financial entity is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.	***deleted***

Article 21 - paragraph 4:

Text proposed by the Commission	*Amendment*
Financial entities shall ensure that tests are undertaken by independent parties, whether internal or external.	***deleted***

Article 21 - paragraph 5:

Text proposed by the Commission	*Amendment*
Financial entities shall establish procedures and policies to prioritise, classify and remedy all issues acknowledged throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.	***deleted***

Article 21 - paragraph 6:

Text proposed by the Commission	*Amendment*
Financial entities shall test all critical ICT systems and applications ***at least yearly***.	Financial entities shall test all critical ICT systems and applications ***on a regular basis.***

Article 21 - paragraph 6 (new):

Text proposed by the Commission	*Amendment*
	After the notification of competent authorities, financial entities that outsource all ICT services to run their business operations may delegate the tasks as set out in the Articles 21 and 22 to intra-group or external undertakings (such as the ICT third-party service provider(s) to whom the ICT services are outsourced to). The management body of the financial entity shall however – in accordance with Article 4.2.(a) - bear the final responsibility for managing the financial entity's ICT risks.

Testing of ICT tools and systems

Article 22 - paragraph 1:

Text proposed by the Commission	*Amendment*
The digital operational resilience testing programme referred to in Article 21 shall	***deleted***

provide for the execution of ***a full range of*** appropriate tests, including vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.	

CHAPTER V - MANAGING OF ICT THIRD-PARTY RISK

General principles

Article 25:

Text proposed by the Commission	*Amendment*
Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the following principles:	Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework***, if any,*** and in accordance with the following principles:

Article 25 - paragraph 3:

Text proposed by the Commission	*Amendment*
As part of their ICT risk management framework, financial entities shall adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in ***point (g)*** of Article ***5(9)***. That strategy shall include a policy on the use of ICT services provided by ICT third-party service providers and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis. The management body shall regularly review the risks identified in respect of outsourcing of critical or important functions.	***F***inancial entities shall adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in ***paragraph 4*** of Article ***4***. That strategy shall include a policy on the use of ICT services provided by ICT third-party service providers and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis. The management body shall regularly review the risks identified in respect of outsourcing of critical or important functions.

Article 25 - paragraph 4:

Text proposed by the Commission	*Amendment*
As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.	***F***inancial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a Register of Information in relation to all ***essential*** contractual arrangements on the use of ICT services provided by ICT third-party service providers.

Article 25 - paragraph 6:

Text proposed by the Commission	*Amendment*
Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with high, appropriate and the latest information security standards.	***deleted***

Article 25 - paragraph 9 - subparagraph 2:

Text proposed by the Commission	Amendment
Financial entities shall ensure that they are able to exit contractual arrangements without: (a) disruption to their business activities, (b) limiting compliance with regulatory requirements, (c) detriment to the continuity and quality of their provision of services to clients.	Financial entities shall ***take appropriate measures to*** ensure that they are able to exit contractual arrangements without: (a) disruption to their business activities, (b) limiting compliance with regulatory requirements, (c) detriment to the continuity and quality of their provision of services to clients.

Article 25 - paragraph 11:

Text proposed by the Commission	*Amendment*
The ESAs shall, through the Joint Committee, develop draft regulatory standards:	***deleted***

(a) to further specify the detailed content of the policy referred to in paragraph 3 in relation to the contractual arrangements on the use of ICT services provided by ICT third-party service providers, by reference to the main phases of the lifecycle of the respective arrangements on the use of ICT services; ***(b) the types of information to be included in the Register of Information referred to in paragraph 4.*** ***The ESAs shall submit those draft regulatory technical standards to the Commission by [PO: insert date 1 year after the date of entry into force].*** ***Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.***	

Article 25 - paragraph 11 (new):

Text proposed by the Commission	*Amendment*
	Financial entities as referred to in Article 3 (39) shall put in place the requirements as referred to in paragraph 4 in accordance with Article 31 paragraph 6 of Directive (EU) 2016/2341.

Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements

Article 26 - paragraph 1 - subparagraph 1:

Text proposed by the Commission	*Amendment*
When performing the identification and assessment of ICT concentration risk referred to in point (c) of Article 25(5), financial entities	When performing the identification and assessment of ICT concentration risk referred to in point (c) of Article 25(5), financial entities

shall take into account whether the conclusion of a contractual arrangement in relation to ***the*** ICT services would lead to any of the following:	shall take into account whether the conclusion of a contractual arrangement in relation to ***important*** ICT services would lead to any of the following:

Article 26 - paragraph 2:

Text proposed by the Commission	*Amendment*
Where the contractual arrangement on the use of ICT services includes the possibility that an ICT third-party service provider further sub-contracts a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such possible sub-contracting***, in particular in the case of an ICT sub-contractor established in a third-country***. Where contractual arrangements on the use of ICT services are concluded with an ICT third-party service provider established in a third-country, financial entities shall consider relevant, at least the following factors: (a) the respect of data protection; (b) the effective enforcement of the law; (c) insolvency law provisions that would apply in the event of the ICT-third party service provider's bankruptcy; (d) any constraints that may arise in respect to the urgent recovery of the financial entity's data. ***Financial entities shall assess whether and how potentially long or complex chains of sub-contracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.***	Where the contractual arrangement on the use of ***important*** ICT services includes the possibility that an ICT third-party service provider further sub-contracts a critical or important function to other ICT third-party service providers, financial entities shall ***appropriately*** weigh benefits and risks that may arise in connection with such possible sub-contracting. Where contractual arrangements on the use of ***important*** ICT services are concluded with an ICT third-party service provider established in a third-country, financial entities shall consider relevant, at least the following factors: (a) the respect of data protection; (b) the effective enforcement of the law; (c) insolvency law provisions that would apply in the event of the ICT-third party service provider's bankruptcy; (d) any constraints that may arise in respect to the urgent recovery of the financial entity's data.

Key contractual provisions

Article 27 - paragraph 1 (new):

Text proposed by the Commission	*Amendment*
	At the date of entering into force of this Directive, existing contracts can be kept unchanged and respected until the termination date, while all new contracts should be in line with these new requirements.

Article 27 - paragraph 2 - point a:

Text proposed by the Commission	*Amendment*
(a) a clear and complete description of all functions and services to be provided by the ICT third-party service provider, indicating whether sub-contracting of a critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such sub-contracting;	(a) a clear and complete description of all ***important*** functions and services to be provided by the ICT third-party service provider, indicating whether sub-contracting of a critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such sub-contracting;

Article 27 - paragraph 5 (new):

Text proposed by the Commission	*Amendment*
	At the date of entering into force of this Directive, existing contracts can be kept unchanged and respected until the termination date, while all new contracts should be in line with these new requirements.

CHAPTER VII - COMPETENT AUTHORITIES

Article 41 - paragraph 1 - point n:

Text proposed by the Commission	*Amendment*
(n) for institutions for occupational retirement pensions, the competent authority designated in accordance with Article 47 of Directive 2016/2341;	***deleted***

CHAPTER IX - TRANSITIONAL AND FINAL PROVISIONS

Entry into force and application

Article 56 - paragraph 2:

Text proposed by the Commission	*Amendment*
It shall apply from [PO: insert date - ***12*** months after the date of entry into force].	It shall apply from [PO: insert date – ***36*** months after the date of entry into force].