Insurance Europe response to the second batch of draft DORA Level 2 measures

Our reference:	EXCO-CS-24-012	Date:	04/03/2024
Related documents:	EIOPA public consultation on the second batch of DORA policy products		
Contact person:	Personal & general insurance department	E-mail:	Fitzpatrick@insuranceeurope.eu
Pages:	28	Transparency Register ID no.:	33213703459-54

This document contains Insurance Europe's response to the consultation on the second batch of policy products developed by the European Supervisory Authorities (ESAs) to complement the Digital Operational Resilience Act (DORA Level 2 measures).

The six consultation papers include draft regulatory technical standards (RTS), draft implementing technical standards (ITS) and draft guidelines (GL), namely:

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

Abbreviations used in the response:

CA	Competent authority
CTPP	Critical third-party provider
DORA	Digital Operational Resilience Act
EIOPA	European Insurance and Occupational Pensions Authority
ESA	European Supervisory Authority
EU	European Union
FE	Financial entity
GL	Guidelines
ITS	Implementing technical standard
KPI	Key performance indicator
LO	Lead overseer
RTS	Regulatory technical standard
SME	Small and medium-sized enterprise
TLPT	Threat-led penetration tests

ANNEX I: Draft RTS on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), (b) and (d) of Regulation (EU) 2022/2554

Q1.	*Do you agree with the content of information to be provided by ICT third-party providers in the application for a voluntary request to be designated as critical? Please, provide comments on information to be added or removed including the rationale (Article 1)*

No

On the content to be provided by ICT third-party providers, Insurance Europe is concerned by the high level of administrative burden this will generate to comply with the request, especially for small and medium-sized enterprises (SMEs). This applies to the content requested in Articles 1, 3, 6 and 7.

The content of the information to be provided by the ICT third-party provider should be aligned with the financial entity's (FE) register of information so that the FE is not required to request additional information from the providers.

Furthermore, it is noted that to establish and keep the register of information up to date will be an extremely time-consuming exercise. Thus, the administrative burden on the FE should be reduced as much as possible, i.e. the ESAs should request all necessary information directly from the (voluntary) critical ICT third-party providers (CTPP) so that the FE can refer to information already received by the ESAs, instead of all FEs requesting the same information. In this way, the FE should only fill in information concerning 'regular' ICT third-party providers in their register of information.

It is not clear what should be understood as 'ICT systems and applications that support critical or important functions'. Further guidance on this would be useful to clarify whether an organisation should approach this from a financial perspective (crown jewels, key applications from the accountant/Solvency II), or the critical systems from a hacker's perspective?

Q2.	*Is the process to assess the completeness of opt-in application clear and understandable? (Article 2)*

Yes

Q3.	*Is the list of information to be provided by critical ICT third-party service providers to the Lead Overseer that is necessary to carry out its duties clear and complete? Please, provide comments on information to be added or removed including the rationale (Article 3)*

Yes

Q4.	*Do you agree with the content of Article 4 on remediation plan and progress reports?*

Yes

Q5.	*Is the article on the structure and format of information provided by the critical ICT third-party service provider appropriate and structured? (Article 5)*

Yes

Q6.	*Is the information to be provided by the critical ICT third-party service provider to the Lead Overseer complete, appropriate and structured? (Article 6 and Annex I)*

Yes

Q7.	*Is Article 7 on competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer clear?*

No

According to Article 7(2)(a), the competent authorities (CAs) must take into consideration the remediation measures implemented by FEs to mitigate risks connected to using a CTPP. It is unclear though how the FE should convey the information to the CAs. Furthermore, it is not clear what will be the administrative costs for the FE to fulfil the requirement. A thorough impact assessment would be appreciated.

Further, according to Article 7(4), CAs can request from the FEs any information necessary to carry out the assessment specified in paragraph 1. Insurance Europe finds it inappropriate to impose an administrative burden on an FE in relation to oversight activities that do not have the FE as the subject.

Q8.	*Do you agree with the impact assessment and the main conclusions stemming from it?*

Yes

Insurance Europe agrees with the assessment that the draft RTS will lead to additional compliance efforts and administrative burden for the FEs as they must invest in new systems and processes to ensure compliance with the requirements in the RTS.

However, the impact assessment is not transparent in relation to the extent of the administrative burden. For example, it is not clear what the remediation measures implemented by the FE would entail.

ANNEX II: Draft joint guidelines on the oversight cooperation and information exchange between the ESAs and the competent authorities under Article 32(7) of Regulation (EU) 2022/2554

Q1.	*For each guideline, do you consider the Guideline to be clear, concise and comprehensible? If your answer is no, please refer to the specific point(s) of the guideline which is/are not sufficiently clear, concise or comprehensible.*

- Guidelines 1-8: Yes

- Guideline 9: No

Further clarification on the term "*other additional information as deemed useful…"* under Guideline 9 would be helpful to support the implementation of the regulation.

- Guideline 10-12: Yes

- Guideline 13: No

It would be helpful if Guideline 13 could include a thorough description of the measures that the CAs can impose on the FEs in accordance with Article 42 and Article 50 in the Level 1 text as well as provide scenarios for the measures. The current wording is unclear, which makes it difficult for the FEs to navigate in relation to the use of CTPPs.

Q2.	*Taking into account the specific scope of these Guidelines, do you consider that these Guidelines cover all the instances where cooperation and information exchange between CAs and the LO is necessary? If your answer is no, please propose additional areas that should be covered.*

Yes

Q3.	*Do you consider that the implementation of these Guidelines will contribute to adequate cooperation and information exchange between the ESAs and CAs in the conduct of oversight activities? If your answer is no, please propose an alternative approach how this could be achieved.*

Yes

Insurance Europe considers this to be true, however, the Guidelines are only concerned with the information to be provided by the CAs to the Lead Overseer (LO). It is equally important to ensure that the FEs are continuously informed about findings/conclusions. In this way, the FEs will be able to take such information into consideration for outsourcing arrangements/processes and ensuring ongoing compliance.

It is important to note that one of the purposes of Article 30 in the level 1 text is to balance the negotiation power between the FEs and the third-party providers.

Q4.	*What are your main expectations regarding the impact on financial entities and CTPPs of the application of these Guidelines?*

It is difficult to determine how the Guidelines will impact FEs and CTPPs. Thus, it would be helpful if the ESAs could provide a more detailed description on the LOs mandate to dictate or enforce a FE's exit from a CTPP if the risk is assessed to affect financial stability.

Also, have the ESAs considered a scenario where some TPPs or CTPPs do not wish to provide their service to an FEs in the EU due to the extensive requirements, and the effect this might have on the FEs and the consequences for financial stability?

ANNEX III: Draft RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

Q1. *Are articles 1 and 2 appropriate and sufficiently clear?*

No

Overall, Insurance Europe holds the view that the proposed solutions in this RTS impose an **excessively burdensome regulatory framework** on FEs, making it impractical to implement, especially in the context of ICT service providers offering standard cloud services not specifically tailored for the financial market.

It is worth noting that standard cloud services often involve a multitude of subcontractors, ranging from a minimum of five to as many as fifty only at the first level, not counting the whole chain. These subcontractors differ significantly in their roles and impact. For instance, some provide critical services like hosting or data connectivity, while others offer auxiliary functionalities such as user interaction analytics.

While Insurance Europe acknowledges the importance of maintaining a registry and imposing obligations on subcontractors that deliver a substantial portion of the contracted ICT service, it appears disproportionate to extend identical regulations to all subcontractors. On the contrary, this approach **could hinder FEs from utilising the majority of standard cloud services**, including widely used solutions such as standard CRM or call centre services, as not all cloud service providers will possess the capacity or willingness to accommodate such stringent requirements, potentially impeding technological advancement within the financial sector.

Therefore, Insurance Europe advocates for a **more nuanced and tiered regulatory approach**, distinguishing between subcontractors based on the criticality and scope of their services to the FEs.

The scope of the RTS should also be strictly limited to material subcontractors delivering an ICT service that is part of the ICT service supporting a critical or important function, as is the case in the register of information on contractual arrangement. The current phrasing is insufficient in terms of legal certainty. This should also be clarified in Article 3. The administrative burden will otherwise be disproportionate, as it would not be relevant for the FEs to conduct such risk assessment and monitoring obligations on all subcontractors including non-material ones.

To limit administrative burden, the broader scope of DORA in relation to the use of ICT third-party service providers compared to existing legislation and guidelines should be taken into account.

Further clarifications are needed on the scope and specific articles, as outlined below.

- Article 1(a): it should be clarified that the parent company only needs to be considered when the ICT subcontractor is not an EU-based legal entity.
- Article 1(b): it should be clarified that this requirement only applies for material subcontractors supporting the service.
- Article 1(c): how should "*the nature of data*" be interpreted? Is there a suggested categorisation of data to adhere to?
- Article 1(f): the meaning of the terms "*transferability*" and "*including as a result of technology specificities*" should be clarified.
- Article 1(h): this concern is limited to vendors that are not designated as critical by the supervisory authorities. In addition, how should the term "*reintegrating*" be interpreted? Is it the level of difficulty for the ICT third-party providers to reintegrate the service that should be assessed or the FE's ability?
- It would be helpful if Article 1 could provide examples on what would decrease or increase risk.

The current wording of Articles 1(f), (g) & (h) leaves room for interpretation as to whether these subparagraphs exclusively concern risks associated with subcontracted services (e.g. potential disruptions caused by subcontractors or the necessity to transition to alternate subcontractors) or if they encompass the entire scope of risks related to the whole ICT arrangement as such. Should the latter interpretation be correct, Insurance Europe would consider it a reasonable approach. However, if FEs are expected to individually assess transferability, disruption risk, and reintegration risk for each subcontractor, particularly in the context of standard cloud services, this requirement becomes unreasonable. Conducting such detailed risk assessments at the subcontractor level is not feasible for FEs due to the complex and multi-layered nature of these services. A more practical approach would involve assessing these risks at the overall ICT service level rather than at the granular level of individual subcontractors.

Article 1(i): it would be helpful to clarify whether 'concentration risk' is the same as the defined term 'ICT concentration risk'. If so, it would be preferable to consistently use the same terminology. Further, it would be helpful to clarify whether the concentration risk is to be considered by firms in the context of their own use of a particular provider, or in the context of the wider sector and the sector's reliance on certain providers within the market more generally. It would also be helpful if the RTS gave some indicative metrics to help determine what may constitute a concentration risk in these cases.

Article 2: as regards group application, it should be clarified that the obligation of the parent company is limited to the scope of the services that are allowed to be subcontracted ("*where permitted*") and is also limited to subsidiaries that are also in the scope of DORA. Further clarification would be welcome on the terms "*adequate*" and "*implemented consistently*" in this article.

The relationship between Article 1 and Articles 2 & 7 should be clarified, for instance what is the exact relation between the elements listed and the obligations of Article 7; should the termination depend on these elements? Such factors should be considered when assessing the risk and/or construing contractual arrangements and therefore be limited to appropriate articles.

Q2. *Is article 3 appropriate and sufficiently clear?*

No

Proportionality is not stressed enough in this article. As previously stated, the provisions should focus on major subcontractors (e.g. hosting service providers) as imposing the same risk assessment criteria on subcontractors that perform relatively minor functions (e.g. analytics or SMS services) would be disproportionate and impractical.

This article suggests that FEs have the authority to approve or deny a third party's subcontracting or alteration of subcontracting arrangements. However, even if the FE decides not to work with the third party, they do not possess legal power to enforce changes to subcontracting arrangements. In practical terms, certain provisions such as step-in rights are not feasible in the context of cloud services. Distinguishing between subcontractors will allow for risk assessments to be tailored and make the process more manageable for the FEs.

Insurance Europe is concerned that the RTS will result in a dilution of the ICT provider's contractual liability, given the fact that the risk assessment will be performed both by the provider and the FE. The required assessment of the subcontractor may thus impact liability of the ICT third-party provider in case of pursuing payment under a liability clause. It is unclear what the outcome would be in a case where the risk assessments of the FE and the provider reach different conclusions.

This article raises confidentiality issues, as the provider might be bound by confidentiality clauses with its subcontractor and hence not be able to share some information. For providers that will be designated as critical and included in the oversight framework, this risk assessment on the subcontracting chain will also be performed

by the authorities. It would be beneficial for FEs to be able to rely on the work that will be done at the authorities' level. The requirements could end up removing smaller actors from the market.

It should be clarified whether these requirements apply only to new contracts or if a risk assessment must also be conducted on the stock. In our opinion, it should apply to new or renewed contracts, but compliance for the stock of contracts should not be expected in January 2025.

It is not clear in Article 3 whether (a) to (i) are to be read as conditions that must be met before a FE is permitted to agree to any subcontracting or if before a FE can make a determination as to whether to permit any subcontracting, they must carry out all the assessments specified in (a) to (i) (but the results themselves do not automatically allow or restrict the use of subcontractor).

In Article 3(1)(b): "*when relevant and appropriate*" should be clarified to define the involvement of the FE in the decision-making process, which should be strictly limited.

Article 3(1)(c): the provider will have several different contracts with several FEs but probably a single contract with its subcontractor. Thus, the contract between the provider and its subcontractor will not be able to "*replicate*" the clauses of all the different contracts the provider signed with the FEs, which will make it very complicated for a FE to determine whether the contract between the provider and the subcontractor can be regarded as "*replicating*" its own clauses or not. Such a requirement should enter into force only once standard contractual clauses are made available. At the very least, this requirement should be strictly limited to the mandatory clauses under DORA.

Article 3(1)(e) is redundant as the obligations under level 1 require FEs to have an appropriate risk management framework. Also, in the absence of a direct contractual relationship between the FE and the subcontractor, the end of the sentence should be deleted: "*to monitor and oversee […] directly.*" The monitoring of a subcontractor will necessarily result from clauses that will be inserted in the contract signed between the provider and the FE, which will not create a direct relationship between the subcontractor and the FE.

In Article 3(1)(i) "*any obstacles*" is too broadly described, as in auditing this may go beyond any party's control. Some limitations may be unforeseen and parts of due diligence duties not reasonably feasible for the FE.

If Article 3 is maintained, it should at least be reworded as follows: [A financial entity shall decide whether an ICT service supporting critical or important functions may be subcontracted by an ICT third-party service provider only after having] "asked information from the ICT Third-party provider on the following."

The subcontractor's "*geographical location*" should be clarified (legal seat or data processing physical location) and one term should be used consistently, either 'location' or 'geographical location.'

The risk assessment in Article 3 fails to capture the essence of an efficient risk assessment, increasing the impact of cyber risks. The likelihood of the materialisation of a risk must trigger a periodical assessment (e.g. a single point of failure) and not the existence of a risk itself (the RTS refers to concentration risks, etc).

Under Article 3(2), it is not clear what time indication "*periodically*" refers to. It should be up to the companies to determine the frequency.

Q3. *Is article 4 appropriate and sufficiently clear?*

No

Linked to the response to the previous questions, the proportionality principle is not reflected enough in Article 4. The contractual requirement should apply only to major subcontractors, not all subcontractors.

It is important to recognise the impracticality of incorporating subcontractor-specific service levels and business continuity plans into contracts with the primary ICT service provider. FEs typically do not have access to such detailed technical information regarding every component of the service being provided. Given that the primary ICT service provider retains overall responsibility for the delivery of the ICT service, requiring FEs to manage these specifics at the subcontractor level is not only unfeasible but also diverts attention from more critical oversight responsibilities. Instead, the focus should be on ensuring that the primary ICT service provider upholds high security standards of service and business continuity, which, by extension, would encompass the performance of their major subcontractor.

Insurance Europe is concerned that the RTS will result in a dilution of the ICT provider's contractual liability, given the important rights that the FE will be seeking to benefit from in the relationship between the provider and its subcontractor (audit rights, monitoring, mandatory contractual clauses...) Notably, some provisions of this Article (4(i)&(j) for instance) raise the legal issue that the FE is not a party to the contract between the provider and the subcontractors and can therefore not have any enforceable rights resulting from this contract.

It is likely that some providers will not be able to compel key subcontractors such as cloud providers to agree to such contractual requirements. This would strongly impact the market. All these new demands that will be made by the FEs in the negotiations will probably increase the prices offered by the providers.

Also, it would not be appropriate to include such provisions in the contractual arrangements for providers that do not intend to subcontract. Instead, the provisions should state that if subcontracting is eligible, the criteria should be implemented in the contractual agreements.

It should be clarified whether these requirements only apply to new contracts or if such risk assessment must also be conducted on the stock. In the light of non-retroactivity and legal certainty principles, it should only apply to new contracts and for stock of contracts when they are renewed. The exercise of review will necessarily have to be spread over time.

This article calls for standard contractual clauses, as is allowed under level 1 DORA. Such clauses would be an essential tool for FEs and providers in the negotiations that compliance with DORA will require. Insurance Europe notes that the alignment between L1 and Article 4 is not clear in the current text.

Clarifications are required on the below:

- Under Article 4(d), it is unclear what is meant by ownership of data and how FEs should interpret this. The confusion exists particularly because of the existence of the concept under other EU legislation (e.g. GDPR) with different objectives.
- On Article 4(f): this will present a significant challenge and may be refused by providers, for instance in the case of web hosting outsourcing this would make their architecture fully redundant.
- Article 4(g) should be limited to subcontractors for which failure might have an impact on the provision of the service supporting a critical or important function. Moreover, does Article 4(g) require the subcontractor to comply with the incident response and business continuity plan of the FE or does it require the subcontractor to have such an incident response and business continuity plan of its own?
- On Article 4(i) the capacity of the subcontractor to respond to these requirements from multiple FEs should be considered. This section should allow for solutions such as pooled audits.

- On Article 4(j): it is unclear if this clause applies to the subcontractor or the ICT third-party provider.
- Some guidance on the risk assessment of jurisdictions would be helpful to include.

Q4. *Is article 5 appropriate and sufficiently clear?*

No

The requirement that FEs should monitor the entire chain of ICT subcontractors, including monitoring key performance indicators (KPIs) and reviewing subcontracting documentation, is highly impractical. This requirement would result in an excessive administrative burden and substantial costs for FEs. Also, it diverts attention and resources away from the more critical oversight responsibilities and managing actual risks.

It is not feasible to monitor every KPI at every subcontractor level. This process is extremely costly and complex, and can be limited by legal obstacles. In practice, the relevance of this monitoring depends on the size (and bargaining power) of the insurance company because smaller companies struggle to integrate penalty clauses in SLAs.

For legal certainty reasons, the monitoring should be strictly limited to the information provided by the provider in accordance with Article 28(3) and (9) of DORA. Firstly, as the owner of the contractual agreement and relation for their chain of subcontractors, it is the provider's role to collect and provide the necessary information to the FE. Secondly, the register contains all the information that the FE is required to obtain under level 1. No additional information gathering requirements should be introduced in the RTS.

Moreover, this requirement should be strictly limited to material subcontractors delivering an ICT service that is part of the ICT service supporting a critical or important function, as is the case in the register of information on contractual arrangement.

On the basis of Article 31(12) of DORA (according to which a subsidiary of a third country ICT third-party service provider designated as critical must be established in the EU), it is not necessary that all subcontractors in the ICT supply chain are monitored. In these circumstances, monitoring should already occur by the national supervisor and should not be duplicated by insurance companies.

The contractual clauses required in Article 4 will not give the FE a legal basis to monitor the whole subcontracting chain and/or review the contractual documentation between providers and subcontractors. Thus, Article 5 provides additional conditions under which an ICT service supporting a critical or important function may be subcontracted.

The conditions set in Article 4 and 5 will be extremely difficult to negotiate with the provider and will contribute to the dilution of the provider's contractual liability. This is why it is key to make available standard contractual clauses and to ensure alignment with other standard contractual clauses available (notably in GDPR).

It seems unfeasible that contracting parties would provide all customers with the ability to review contractual agreements with underlying suppliers. There are also legal obstacles to performing such a review because many contracts include confidentiality clauses. However, transparency should be provided so that this could be incorporated into risk analyses and agreements regarding SLA/in-control status.

Finally, Article 5(2) raises a legal issue and should be limited to contractual documentation relevant for the quality of service strictly related to the critical and important service deliveries.

Q5. *Are articles 6 and 7 appropriate and sufficiently clear?*

No

Articles 6(3) and 6(4) are not feasible to implement as they fail to consider the practical reality behind these services. Regarding confidential entities, if a subcontractor changes, they may need to align with multiple FEs which may not be feasible. In some contexts, prior approval is not feasible, e.g. when a subcontractor changes location (because of new building regulations or reorganisations), the prior approval by the FE is not feasible. This requirement could lead to a scenario where a third-party provider is unable to make a change without the approval of all financial services clients. This could be more easily implemented if standardised contract clauses and standardised due diligence frameworks were created, and pooled audits allowed.

Articles 6(3) and 6(4) also present a significant challenge when applied to standard multi-tenant cloud services. In such scenarios, it is impractical for a single customer, even if it is a FE, to exercise influence over or restrict the technological advancements of large cloud ICT service providers, such as Microsoft. The expectation that a FE could effectively object to or require changes in subcontractors within these complex cloud environments fails to consider the practical realities of how these cloud services operate and evolve, especially in a market dominated by major ICT players who serve a diverse and extensive customer base.

Article 7 will also be very challenging to negotiate with major providers, which are not regulated entities and do not have any obligation to accept this kind of requirements.

It is not clear if Article 6 only refers to material changes in subcontracting arrangements for ICT services supporting critical or important functions. As mentioned before, the scope of Article 6 should be limited to cover material subcontractors only.

FEs should not be required to share risk assessments with their providers, thus Article 6(2) should be deleted. It may not only contain confidential information, but also could impact contractual agreement negotiations.

It would also be important to ensure general consistency with EIOPA's Guidelines on cloud outsourcing, and in particular to give effect to Guideline 13 on the sub-outsourcing of critical or important operational functions or activities. Paragraph 50(e), for example, provides that where a cloud service provider plans changes to a sub-outsourcer or sub-outsourced services that would have an adverse effect on the risk assessment of the agreed services, that the insurance undertaking has the right to object to such changes and/or the right to terminate and exit the contract. Paragraph 50(c) also specifies that the cloud service provider should retain full accountability and oversight for the services sub-outsourced.

Insurance Europe would suggest adding the possibility for the FE to terminate the contract if the provider does not provide the required information in accordance with Article 28(3) and (9) of DORA. Also, to add a notice period after a material change, in order to allow the FE enough time to assess the risks.

In Article 7(1)(a) it is not clear whether a tacit approval is permissible (i.e. based on contractual provisions, no information given to the provider within a specified time may be understood as approval). Further under 7(1)(b) the term "*explicitly*" is not clear. It should refer to subcontracting against the rules set out in the contractual agreement. The subject of the subcontracting may be an element of the service that is permitted to be subcontracted. In such case, it is not clear whether the subcontracting is (based on commented provision) allowed or if the agreement should be terminated (based on the assumption that such "element" was not indicated "explicitly")

Under Article 7, does "*terminate*" equate to annul or rescind with no penalties/immediate effect, or is it right of withdrawal? How does this technical provision relate to the principle of 'pacta sunt servanda'? More generally, the provider will undoubtedly want to calculate their risks and burdens, which will become an important factor in (re)negotiations with FE, included in pricing schemes.

Q6. *Do you have any further comment you would like to share?*

Insurance Europe notes that the proposed RTS requirements extends beyond the current Solvency 2 requirements governing outsourcing of critical or important functions, and that this creates an **inconsistent approach** between risk management for ICT services supporting a critical or important function and non-ICT outsourcing of critical or important functions.

It is further noted that, in almost all cases, FEs do not have a direct contractual relationship with subcontractors used by ICT third-party service providers, and hence have no legal right to impose requirements on them or carry out many of the proposed draft RTS requirements (privity of contracts). This legal right and a requirement for FEs to vet subcontractors would create a risk of dilution of the responsibility of the ICT third-party service provider and limit the effectiveness of liability clauses as a risk transfer mechanism. The measures proposed should focus on increasing transparency without reducing ICT third-party providers' liability.

The terms of this RTS make complex and costly demands on third-party providers and FE, which need to be eased by introducing standard legal clauses and pooled assessments/audit where possible.

It must be noted that some of the clauses that apply to large IT suppliers are difficult to adapt for smaller or medium-sized companies.

If a provider has already been submitted to oversight under 41(1), then the authorities already have certain information that could lighten the subcontracting reporting under this RTS.

ANNEX IV: Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

Q1.	*Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.*

No

Several types of costs require clarification and/or are problematic. Some types of losses are captured regularly by the sector, but some such as "*business-as-usual costs*" referred to that would include productivity loss are not currently captured. It is unclear what these specific costs entail, and it would add administrative burden for FEs to collect them. It is also not clear whether the losses should also reflect marginal losses.

It is unclear how costs (e.g. relocation costs) should be added to "*losses due to forgone revenues*". The reason being that costs should logically be compared to loss of profit, rather than loss of revenues. If that is the intention of the lawmaker, then this should be made clear in the Guidelines. It should be clarified if it is the profit margin of the foregone revenues that should be added to the costs.

Some of the suggested cost categories will be rather difficult to estimate with reasonable accuracy, e.g. costs for "*impaired skills of staff*" and "*costs associated with internal and external communication*". Insurance Europe suggests that it is made clear that these costs can be provided as rough estimates.

Further clarification would be welcome on how the proposed Guidelines will work with other incident reporting requirements, e.g. data privacy. Also, it should be clarified how multi-year costs are treated, and what happens when the incident and recovery losses accounting year ends.

Paragraph 9 of the Guidelines stipulates that adjustments on the costs and losses reported in the aggregated reporting of a previous year should be included in the reporting of the relevant accounting year in which the adjustments are made. It is understood that the Guidelines refer to accounting and adjustments to financial aggregated reporting, which goes beyond the mandate of this text.

The report requested on major ICT-related incidents involves a report to the regulator. If changes to financial reporting are necessary, they should be determined within the framework of national accounting legislation, with statutory reports following the rules of the accounting decree and consolidated reports following IFRS rules.

Besides this, the application of the principle of proportionality is based on incorrect assumptions, i.e. that smaller companies are less likely to classify ICT-related incidents as major. Smaller companies are more likely to classify ICT-related incidents as major, given their more restricted control environment, with proportionally more Single Points of Failure and fewer mitigation options.

Q2.	*Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.*

No

Regarding costs related to major ICT incidents that occurred in previous years and that had a "*quantifiable financial impact on the validated financial statement [...] in the relevant accounting year*" (in the rationale under

Title III, 6(b)), it can be interpreted that all costs should be reported, no matter how limited. Insurance Europe suggests that a threshold is applied, so that the costs that should be reported are of a reasonable size.

In paragraph 8, "*…and that, if legally required, are validated by an independent entity*" is considered unnecessary and could be removed.

Regarding paragraph 8, it would be welcome if the ESAs could provide expectations/examples on how the estimation is to be reflected in the annual report.

Q3.	*Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.*

No

Insurance Europe finds it disproportional that the FEs are to report both aggregated data as well as data for each individual major incident. This requirement adds extensive administrative burden on the FEs.

It would be helpful if the ESAs could convert the proposed template in the annex into an online platform, where the FEs can report the estimates as well as access previous reports, which would help alleviate some of the administrative burden.

The task of qualifying some elements for VAT on costs incurred, and especially losses, may be burdensome (as regards breakdown of costs and losses into net and gross values).

It must be further noted that it is impossible to determine the exact "*economic impact*" cited in the Guidelines. This will always be provided on a best estimate basis.

Q4.	*Do you have any further comment you would like to share?*

The Guidelines are not in line with any standard accounting practices. This creates confusion, difficulties in implementation and legal uncertainty. It should be aligned with accounting practices/existing standards and legislation on the matter.

Further, the mandate of the Guidelines is limited to the estimation of aggregated annual costs and losses in the context of incident reporting. It should not cover accounting rules for the purpose of drafting financial statements.

It is unrealistic to expect that FEs can make accurate estimates of gross and net losses. This will be especially challenging for smaller FEs that do not necessarily have functions that are used to working on this type of task. Consequently, there is a risk that the figures provided will be inaccurate and thus less usable.

ANNEX V: Draft RTS on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and draft ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat

Q1.	*Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.*

No

Insurance Europe has strong concerns about the proposed tight unfeasible timelines, which risk distracting the financial entities (FEs) from managing incidents by forcing early reporting.

The architecture of criteria to classify an incident as major is complex. The classification requires information to be gathered from numerous stakeholders when an assessment of the 'other criteria' (clients, financial counterparts and transactions, data loss, reputational impact, duration of service downtime, geographical spread, economic impact) is required. This exercise will call for a high involvement of different teams (notably IT, security, crisis management business, DPO, Risk, etc.) and will be even more challenging in a cross-country and cross-organisation environment, for instance when FEs have several subsidiaries or when the incident originates from a provider.

Availability of the staff is limited. The FE will need to collect information from various sources within the entity and from business partners that might not work over the weekend. Similarly, the team usually responsible for the classification and the reporting itself does not work 24/7. This organisational issue will be even greater for small and middle-sized entities. Any communication of this type may need to be signed off by the executive team, which also needs to be factored in.

This short timeline could thus lead to a significant amount of major incident notifications that would need to be requalified afterwards as non-major. Such wrong classifications based on an incomplete analysis or on poor quality data would entail administrative correction afterwards, which would create unnecessary administrative burden both for FEs and authorities. FEs' resources should prioritise solving the major incident.

Stakes of the insurance sector are different from those of payment services. A 4-hour time limit is aligned with PSD2 but does not fit with the insurance sector. Indeed, the insurance sector does not have functions that are critical on a 4h or even a 24h basis. Underwriting and claim managements, should they be regarded as critical, can be delayed for more than 24 hours without causing damage to the company, the clients and/or its business partners. In this regard, it must be stressed that level 1 DORA encourages the ESAs to provide different timeframes for different sectors[1]. There should be no 4-hour time limit.

It does not seem relevant to align timelines with Directive 2022/2555, considering the entities included in the scope of DORA will not apply it. However, it is noted that the timeline proposed in this RTS is even shorter than that of Directive 2022/2555 which requires only an "*early warning", "without undue delay and in any event within 24 hours of becoming aware of the significant incident*". This phrasing should be reflected in the RTS to

[1] "*take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations,* ***and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, specificities of financial sectors****, without prejudice to maintaining a consistent approach to ICT-related incident reporting" pursuant to this Regulation and to Directive (EU) 2022/2555*". (Article 20(a)(iii))

align with the NIS2 Directive. It would be appropriate to align the timelines with the other notification obligations for FEs subject to DORA such as the GDPR.

An **adequate timeline** that would also allow for an effective notification process for the insurance sector would be the following:

Initial notification submitted within 24 hours after classification and if the incident occurs on a weekend day or a bank holiday in the member state of the reporting FE, the notification should be filed within the next working day. The requirement to file the report within one hour following "*regular starting time*" of the next working day when the deadline falls on a weekend day or a bank holiday is vague and in practice too short to comply with.

Intermediate report submitted within 10 working days of the initial notification. The 72-hour time limit for the intermediate report is insufficient, especially considering the data to be filed at this stage and the fact that the FE will still probably be in crisis mode. Moreover, if the intermediate report is filed within 72 hours after the classification of the incident, and updates are required under level 1 each time there is a relevant status change in the incident, it may result in a high stream of notifications to the authorities.

Final report submitted within 30 working days of the "*permanent resolution*" of the incident, which is to be understood as including the recovery of the business services and the root cause analysis required by level 1 but excluding any long-term action plans. This would give the FE enough time to restore the services, identify the root cause and draft the report.

Further clarification is needed on the following terms:

- "*Detection*": an incident can be detected by one user, without immediate identification of impacts and therefore qualification of the incident as major is not feasible. Identification of an incident as major might take more than 24 or even 72 hours. Using "*detection*" as a starting point will probably encourage overreporting by the FEs.
- On the timeframe applicable to the intermediate report, the RTS should clarify that the terms "*Regular activities have been recovered and business is back to normal*" mean business service recovery.
- "*Resolution"/"permanent resolution*": in the final report, the ICT incident can be resolved through a work-around, while resolving the root cause of the incident takes more time. Actions and measures taken to permanently resolve the incident are part of the long-term action plan, which corresponds to other DORA level 1 obligations, such as requirements set in Article 13 "*learning and evolving"*. Insurance Europe strongly recommends limiting the notion of "*resolution/permanent resolution"* to business service recovery and identification of the root cause.
- In Article 6(1)(c), either "*resolve*" or "*permanently resolved*" should be used but not both without explaining the difference between the two situations.

Q2.	*Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.*

No

As stated in the earlier question response, the timeline of 4 hours is not feasible.

Article 3 contains **several data fields that should be removed and instead included in the intermediate or final notification** as the information will not immediately be available. This includes paragraphs (d), (e), (g), and (h), especially the latter on recurring incidents where this will require cross-referencing several incidents and divert resources from resolving the incident. Alternatively, should these fields be maintained in the initial

notification, it should be required only "*where available and applicable*" and with the option of completing them in a subsequent notification if it is more appropriate.

Regarding the content of the annex, Insurance Europe suggests the following modifications and/or clarifications to avoid confusion and to promote legal certainty:

- 2.3 - Incident description: it should be clarified whether the recurring incident details should be included in this field, considering that there are other dedicated data fields for recurring incidents. Additionally, it will be challenging to explain the internal severity assessment conducted by the FE at this stage. This should be moved to the final report or removed.
- 2.6, 2.7 and 2.8 - Information about the source of the incident: Considering the proposed time limits defined for the initial notification (i.e. 24h/4h), FEs are unlikely to know where the incident is coming from before the investigations are completed unless the providers inform them.
- 2.11 - Recurring incident: A clarification is required to define when an incident should be considered as a recurring incident from a security incident perspective.

Insurance Europe agrees with the need to share information swiftly to avoid spill-over effects. However, the current information requested and template in appendix demands too much time for an organisation that is in the midst of addressing a serious issue. Part of the information requested is already known to the ESA, such as name of the organisation, LEI and contact persons. It would be useful to enable the sharing of this general information continuously or separately from the incident with the authority (preferably through a dedicated online platform) so that in the case of the incident, only specific incident-related information would have to be shared.

In terms of submitting the initial notification, it is not clear who is allowed to report to the ESA, whether on a group level or unit level. To limit the reporting burden, Insurance Europe would suggest a single report be provided for a company on a group level if the incident is affecting multiple units. This is also related to reporting losses.

Q3.	*Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.*

No

As stated in the earlier response, the timeline of 72 hours is not feasible as it does not grant the FEs enough time to reflect material change and supply the information requested whilst addressing the incident itself. This deadline is particularly tight when several member states are involved. It will also be very challenging to provide parts of the information specified in the intermediate report within 72 hours, e.g. "*Information about affected functional areas and business processes*" and "*Information about affected infrastructure components supporting business processes.*"

The mandatory reporting should not pose a significant burden. This is clearly mentioned in reference to the voluntary notifications, but the same logic is not observed with the mandatory reporting. Insurance Europe would welcome if the ESAs could apply the same rationale to the mandatory reporting, with a view to limit the reporting requirements in accordance with the political wish to reduce reporting requirements by 25 % as formulated by von der Leyen during her State of the Union speech on 13 September 2023.

Regarding the content of the annex, Insurance Europe suggests the following modifications and/or clarifications to avoid confusion and to promote legal certainty:

- 3.5 - Date and time when services, activities and/or operations have been restored: the recovery of the service should be understood as business recovery.

- 3.26 - Type of incident, 3.15 and 3.16 on reputational impact: this is more relevant in the final report because at this stage, it is still early to confirm. We suggest removing this field from the intermediate report and move it to the final report.
- 3.27 - Threats and techniques used: We encourage mapping this field with MITRE ATT&CK, which is a well-known framework to FEs. Moreover, this field should be transferred to the final report as this information will not be available at this stage.
- 3.36 & 3.37 – Temporary actions: it should be clarified whether this field would include manual workarounds for business or temporary IT/security fixes.
- 3.38 & 3.39 – CSIRT involvement: it should be clarified whether this field refers to the internal CSIRT or only the external CSIRT. In all cases, we wonder about the added value of this information for the authorities. We suggest removing this field or at least moving it to the final report, as an area for improvement in case no CSIRT is in place.

Further clarifications required related to the intermediate report:

- Article 4(b) "*Date and time of occurrence of the incident*" should be moved to the final report. The occurrence of an incident might require forensic analysis, and therefore it may not be identified before the intermediate report is required to be submitted.
- Article 4(d) and 4 (e) can be removed as these pieces of information are redundant/unnecessary as the initial notification will already contain these according to Article 3.
- Article 4(f) and 4(g) is information that will be challenging to provide within 72 hours. If this timeline is maintained, it should be clarified that these data fields are provided on a best-effort basis.
- Article 4(k) and 4(l) should be moved to the final report as it requests information on vulnerabilities exploited and indicators of compromise, information that cannot be available on a short notice.
- In Article 1(a), it should be clarified if "interim report" is the same as "intermediate report." A consistent use of one term should be used throughout the RTS to avoid confusion.

Q4.	*Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.*

No

The deadline to submit the final report no later than one month after the incident or one day after closing is unrealistic. Given the FE's focus will be on resolving the incident, and that the incident may take a month to solve, the company will not be able to prepare the report whilst solving the incident. Further leeway should be given so that the company can focus exclusively on resolving the incident and then have enough time after this date to submit the final report and all necessary data (e.g. including the root cause, which will not be able to determine with the current strict timeline).

Regarding the content of the annex, the following clarifications are needed to avoid confusion and to promote legal certainty:

- 4.3 – Root cause: the root cause identification can be included, however not the long-term action plan meant to treat it.
- 4.6 – Description of measures: the measures and actions taken for the permanent resolution of the incident are also part of the long-term action plan, and not the incident resolution. This field would in practice include change, which can be a long-tailed process and is part of other level 1 obligations under DORA that do not require reporting. It should be limited to measures and actions taken to restore business service and identify the root cause.
- 4.9 – Permanent resolution: similarly, a clarification is needed on what "*permanent resolution*" means. The complete resolution of the problem could be several weeks or even months later as part of a long-

term action plan. We suggest limiting it to the business services recovery and the identification of the probable root cause.

- 4.18 to 4.24 – Amounts: these figures cannot be provided 1 month following the detection of the incident and notably the financial recoveries. These amounts should be provided in the relevant yearly report for the competent authorities rather than in this unitary incident report. In any case, these amounts should be strictly limited to extraordinary costs and not include internal operating costs.

Q5.	*Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.*

No

The wording in Article 7 should be revised to further clarify that this reporting is not mandatory and only done on a voluntary basis. In its current form, the wording does not immediately suggest that it is voluntary. Further, as the FE might not yet have the final information about costs related to the incident, it should be specified that the information requested can be provided as an estimate.

There are existing local communities (e.g. in France: ANSSI, CERTFR) where FEs can share information on cyber threats. To avoid redundant work from FEs, competent authorities could rely on existing communities.

Q6.	*Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.*

No

Where an incident affects several entities of a group, Insurance Europe believes it should be possible to file a single consolidated report, drafted and filed by the parent company or the company that provides the service. The filing of several reports increases the administrative burden of the FEs, without necessarily providing additional information to the authorities. This would allow for a harmonised approach within a group.

It would be preferable if the report could be filed in any chosen language including English to the competent authorities. English is the default language in many international companies. The need to translate for the regulator could impact the reporting speed and report delivery.

It is noted that the secure channels to perform the reporting are not yet described, but it must be kept in mind that they will impact the notification process greatly. These channels must be easy to use, so that FEs can use it even when operating in degraded mode. It would be best to have a standardised reporting template shared between ESAs and a centralised portal/process to submit the reports.

Q7.	*Do you have any further comment you would like to share?*

Article 1 requires the FE to provide the contact details of the contact person responsible for communicating with the competent authority. In our opinion and for operational reasons (absence, position changes), the contact details should be linked to a job function rather than to a person.

It would be useful in the drafting process to consider the work of the Financial Stability Board on the Format for Incident Reporting Exchange (FIRE).

On the wording of the timelines, please align the wording between the time from classification or the time from detection of the incident, as for the moment both terms are used in an unclear manner. See our response to the earlier question on our suggested approach.

Clarification is needed on how to interpret "*significantly*" from the consultation rationale paragraph 16, namely "...*an intermediate report shall be submitted by FEs as soon as one of the below triggers have been met: - as soon as the status of the original incident has changed significantly*".

The reporting currency should be agreed, with two currencies at most being used (local currency and EUR for the purpose of comparability where applicable). The exchange rate of the costs estimate could be based on the rate from the day of the incident.

ANNEX VI: Draft RTS on specifying elements related to threat led penetration tests (TLPT)

Q1.	*Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as needed.*

Yes

The cross-sectoral approach depends on the scoping of the scenarios that are mandatory for testing. Not all scenarios may be relevant, e.g. transaction payments which are mainly relevant for banks.

It should be noted that the entity-agnostic and sector-agnostic methodology and process may be justified from the ESAs perspective but it will require more adjustments on behalf of the insurance sector than of the banking sector.

Also, the RTS places a much greater burden on FEs from member states which have chosen not to implement the TIBER-EU framework. These entities are adversely affected by a member state's non-compliance with rules that had not been set out as mandatory by EU legislators. Perhaps FEs from these member states could be granted some leniency in this respect, i.e. time extension to fulfil duties arising from the RTS, not DORA itself.

Q2.	*Do you agree with the proposed approach on proportionality? If not, please provide detailed justifications and alternative wording as needed.*

No

On the following statement "*Since all financial entities that are required to perform TLPT must meet a high level of ICT maturity*": the concept of maturity should be clarified. Moreover, this criterion will become less and less relevant as DORA will require a common level of cyber resilience.

Article 2(3) does not appear to be proportional in the sense described in point 3.3.2. of the consultation paper as it will allow for application across most participants in the financial services market instead of focusing, as announced, on "*financial entities that carry a certain degree of systemic importance and are mature enough*."

Regarding recital 22, a clarification should be added stating that for every third test, **"only"** external testers shall be contracted, as it is understood that a team of internal and external testers would be considered as a test performed solely by internal testers.

a. Approach on the identification of financial entities required to perform TLPT

Q3.	*Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.*

Yes

In theory, Insurance Europe agrees with the two-layered approach. It is very important though to ensure that only FEs that play a systemic role will be part of the DORA TLPT set-up. It is not clear whether this is the case in the current wording. It is also currently unclear how the ESAs will ensure uniformity across the Union and ensure the cooperation of TLPT authorities with potentially different approaches.

Article 2(2) states that member state authorities will decide whether it is relevant for entities belonging to the same group, meeting the criteria, and using common ICT systems or the same ICT intra-group provider, to

perform a TLPT on an individual basis. In our opinion, in this kind of situation a group TLPT should be favoured with the possibility for TLPT authorities to require otherwise. Thus, if a subsidiary belonging to a group is required by its national authority to perform a TLPT, the entity and the parent company should automatically be given the choice to perform the TLPT at group level, if appropriate.

Indeed, in practice a TLPT does not apply to "entities" *per se*, but rather to ICT systems and services, which are often shared between a group and its subsidiaries. A TLPT would therefore benefit all the beneficiaries of the ICT systems and services, whether they belong to the same legal entity or not. Group level TLPTs should therefore always be a preferred option, except where a subsidiary that meets the criteria has independent ICT systems and/or business particularities that require performing a TLPT on an individual basis. When the TLPT is performed at group level, it should be specified which TLPT authority will be in charge, preferably the competent authority of the group member state.

Insurance Europe fears that this RTS will lead to a broader scope than level 1 in terms of frequency of tests and critical functions tested.

Q4. *Do you agree with the proposed quantitative criteria and thresholds in Article 2(1) of the draft RTS to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.*

No

Insurance Europe agrees that only FEs of certain systemic importance should be required to perform TLPT. Unlike disruptions to the banking system, disruptions related to non-life insurance and reinsurance do not result in such significant impacts to the financial sector nor generate such financial stability concerns that would justify any non-life insurance and reinsurance undertakings to be included by default. Thus, non-life insurance and reinsurance undertakings should not be included in Article 2(1) and shall only be required to conduct TLPT if the TLPT authority assess that it is relevant according to Article 2(3).

For other types of insurance and reinsurance undertakings, the thresholds should be increased to reflect the impact on the financial sector that a disruption in such insurance or reinsurance undertaking would have and possible financial stability concerns. In this regard, it should be noted that insurance and reinsurance undertakings that would not be required to conduct TLPT would still be subject to extensive requirements on digital operational resilience as set out in DORA, including requirements on penetration testing and other tests.

The current provisions under Articles 2(1)(g), 2(2) and 2(3) do not sufficiently clearly and objectively communicate which companies are in scope of TLPT testing. The issue arises from the fact that the information to calculate assets according to the current clauses is not publicly available (if available). This lack of clarity of who would be in scope has serious consequences for FEs as they are unable to prepare for a TLPT and gather the resources and competences needed to perform such tests.

Quantitative criteria given in absolute amounts are not proportionate by nature and percentages should be favoured. For instance, 500 million GWP seems too low for some markets and therefore not proportionate. In this respect, it must be kept in mind that conducting a TLPT is a very costly exercise (around 500k on average for 10 to 12 weeks of testing, which does not fully represent the total cost of the TLPT which also includes a threat intelligence phase and mobilises resources).

Under Article 2(1)(g), it is not clear whether the criteria applies to activities within a given member state, or if it should also encompass the value of the company activities outside the member state. This could lead to very different results in calculating which companies are in scope.

Under Article 2(1)(g)(ii), does the criteria apply to the previous financial year, or to each of the previous two financial years as is the case for point (i)?

Under Article 2(1)(g)(ii), it is not clear whether this refers to the top 10% of the sum of total assets, or to the overall assets linked to one activity area. If it refers to the type of activity areas identified in the earlier clause, this could be problematic to calculate as the information necessary to calculate this is not disclosed (to national bodies, nor supervisor) as the reporting does not include balance sheets by activity – but only one unified sheet. It would only be possible to breakdown the assets in the field of investments, and only for those directly linked to specific activities.

The relationship between Article 2(1)(g)(i) and (ii) is not sufficiently clear. Must a company be in the 10th decile for each of the listed activities and their GWP be above the average GWP for all companies to fulfil criterion (ii)? Or on the contrary does the criteria request that a company's GWP for all the listed activities must be above the average GWP and at the same time the company must be in the 10th decile of all companies to fulfil criteria (ii)?

Article 2(1)(g)(ii) SLT and NSLT are not appropriately defined. It would be better phrased as: "Health-Similar-To-Life (SLT)" and "Health-Similar-To-Non Life (NSLT)". Also, the reference to reinsurance (in the first two bullet points) can give the impression that reinsurance shall be excluded instead of the other way around.

Article 2(2) (second sentence) only includes FEs belonging to the same group on the basis of the criteria in paragraph 1(a) to (g). This excludes groups which consist of IORPs and/or IORPs and insurance undertakings since IORPs are assessed of the criteria listed in Article 2(3). The paragraph should be revised to cover any FE. Where more than one FE belonging to the same group meets the criteria set out in points (a) to (g) of paragraph 1 or paragraph 3.

Under Article 2, the TLPT authority can opt-out organisations from TLPT. It is not clear what are the requirements and criteria a TLPT authority will use to make this decision, or what company considerations will be taken into account (e.g. maturity level? This refers to an earlier need for clarification about how to define and measure this.)

b. Approach on the testing: scope, methodology, conclusion

Q5.	*Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions.*

No

The current approach is sufficient. No further obligatory requirements from the TIBER-EU framework should be included, especially as this has only been implemented by some member states.

Q6.	*Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT? If not, please provide detailed justifications and alternative wording as needed.*

No

In case of a real-world attack during TLPT, a company should be able to pause the TLPT to have the red team focus on solving the current issue. For the moment this is not possible.

Though performing a risk assessment is valuable, it may lose some of its significance if confidentiality constraints imposed by the TLPT practice limits the sharing of its outcomes throughout the FE. The risk assessment should be shared within the FE on a need-to-know basis before the test and shared broadly throughout the FE after the TLPT is conducted.

In point 3.2/19, a mandatory purple team is mentioned, but it seems to be missing from Point 3.5.1/32 "*TLPT participants*." It is recommended that the purple team activity be conducted during DORA. Additionally, the requirement lacks details on what methodology should be used (e.g. scope) for the risk assessment that must be performed prior to TLPT.

Q7.	*Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed.*

No

Article 26 of DORA does not give the ESAs a mandate to detail the criteria set in level 1 for external testers, which seem sufficient and appropriate. Notably, level 1 already requires using testers that are certified or adhere to a code of conduct or an ethical framework (Article 27(1)(d)). Instead of adding a minimum experience criterion, Insurance Europe would suggest adding an approved list of certifications that the entities could base their selection process on.

The minimum experience for external testers is too high. This will increase tensions and create a shortage of profile availability on the market, in a field where experts are often young and potential conflicts-of-interest might prevent entities from using some testers. Similarly, the number of references is too stringent, and it is unclear how these references will be validated without revealing information about the previous assignments. This context is likely to constitute a major practical obstacle to the implementation of TLPTs. Therefore, alternatively, we suggest making "*years of experience*" and "*references*" a recommendation rather than a mandatory criterion in order to offer more flexibility to the FEs.

On this issue of profile shortages, Insurance Europe suggests addressing through the RTS the situation where an entity is required to perform a TLPT but does not find available testers that meet the required criteria in the relevant period. This RTS should provide a possibility to postpone the process with the approval of the TLPT authority until available testers that meet the criteria can be identified.

There is no formal accreditation for TLPT and TI providers. This accreditation should be centrally managed and prevent the different certification requirements of pentesters (Appendix 6.1 in the procurement Guideline). Most of the certifications listed are not relevant. For example, OSWP is only relevant when testing wireless networks, CISSP is too general to perform pentests, whereas OSCP is very relevant.

It would be worth clarifying if the ESAs studied the market to identify the number of skilled people that meet the criteria, in order to set the thresholds of required experience and guarantee TLPT can be run in compliance with DORA.

Q8.	*Do you think that the specified number of years of experience for external testers and threat intelligence providers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills? If not, please provide detailed justifications and alternative wording as needed.*

No

In addition to the earlier response, Insurance Europe seeks to underline that requiring a certain number of years of experience can add unnecessary pressure for highly skilled individuals. These thresholds require further market and impact analysis and should not be mandatory criteria but rather recommendations. Overall, the set of expectations for internal and external testers outlined in Article 5(2)(d) will create a high entry barrier for external testers, which may cause a deficit in the market and also drive up the costs associated with conducting these types of tests.

Red teaming should consist of multiple pentesters. Not all pentesters need to have a specified number of years of experience. Some new pentesters can find vulnerabilities that experienced testers have not looked at. In our opinion, this is not a good measure and it is an unnecessary obstacle for talented people and IT-providers. Especially if there is an accreditation, this point is no longer relevant.

Q9.	*Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed.*

No

In total, as currently provided in the RTS, the proposed testing process will last potentially more than a year. In our opinion, to avoid excessively extending the duration of this process, a maximum duration for the threat intelligence and red team test phases might be more appropriate rather than a minimum duration of 12 weeks for the active red team testing phase.

For proportionality purposes, the duration of the active red team test phase should be determined by the entity itself with the approval of the TLPT authority, based on the criticality of the systems tested and its maturity. At the very least, the minimum duration should be no longer than the duration set in TIBER-EU.

Expectations for purple teaming and tests need to be clarified, particularly regarding the scope of engagement, the frequency, and coordination with other teams. Clarification is needed on the relevance of Article 8(11) which allows the repeat of specific parts of the TLPT and/or carrying out purple teaming exercise at any given time during the active red team testing phase, considering the lack of awareness of the blue team and the potential resource constraints 'unplanned activities' availability on the part of the blue team. It should be at the end of the exercise.

The RTS should provide a longer notice for the blue team report, roughly 8 weeks to allow proper resource planning.

The delay for the remediation plans in the closure phase (i.e. 16 weeks) is too short. This deliverable is one of the most important in the TLPT exercise and must be a 'minimum deadline'. The 16 weeks time limit for the remediation plan should only be applied to critical findings that require a high-priority mitigation. Regarding Article 10(1), it should be noted that Red Team assessments often produce findings that are much more complex to mitigate than findings from e.g. isolated application penetration tests (for example there are often numerous dependencies with surrounding systems that need to be considered for the remediation). It would therefore make sense to set a longer deadline for the creation of the remediation plan.

On the process, most companies already have threat intelligence services. This can be used to select relevant scenarios and does not have to be part of the process, if an FE already has threat intel services running.

Every report must be treated as confidential by all parties as it will contain sensitive information. This should also be requested from the regulator and TLPT parties to ensure the confidentiality of the information.

Red Team Assessments are a major undertaking and consume a lot of resources that might be difficult to develop for the TLTP authority and the FE.

Article 7: It should be stated clearly that the general threat landscape provided by the corresponding TIBER-EU unit is an appropriate basis for the targeted threat intelligence report.

Article 7(3): Insurance Europe considers that two scenarios should be sufficient.

Article 8(10): ICT third-party service providers should be considered when deciding on a test suspension. Recommended wording: "*Under exceptional circumstances triggering risks of impact on data, damage to assets, and disruption to critical or important functions, services or operations at the financial entity itself, its counterparts, ICT third-party service provider or to the financial sector...*"

Q10. *Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.*

No

Insurance Europe encourages pooled testing, since performing a TLPT is not without risk. However, it may generate significant administrative burden for FEs. Therefore, the RTS should provide wider requirements for pooled testing. For instance, an industry-wide infra testing of critical service providers would avoid the exercise being done individually for all undertakings, overburdening the providers and generating additional costs to undertakings without any benefit.

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

Further clarification is needed on the requirements regarding the use of the same pooled testing exercise between different FEs within the same group, particularly when it comes to shared critical business functions provided by an internal IT service provider. Would performing one pooled testing exercise and sharing it among FE of the same group be sufficient? What criteria and rationale would allow for the aggregation of critical business functions and enable sharing of pooled testing among FEs? For instance, if a provider is identified as critical for all entities, would it be feasible to perform a single TLPT for all entities?

c. Approach on the use of internal testers

Q11. *Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.*

No

The criteria for in-house testers are too restrictive and will make it difficult to use in-house testers, especially as this is a field with a very high turnover. As mentioned in the earlier response, the market for external testers is also very tight and the combined requirements for in-house and external testers is likely to constitute a major practical obstacle to the implementation of TLPTs.

The RTS requires that all members of the internal test team have been employed by the FE or by an intra-group service provider for the two preceding years. The reason for this requirement is unclear, as external testers are

not required to have specific knowledge of the FE itself. Moreover, this requirement makes it impossible to reinforce an internal red team in case one member quits. This requirement should therefore be removed or, at the very least, the requirement to have been with the company for two years should be limited to a single member of the testing team (Article 11(a)(ii)). In the event that a red team is not available on the market, it needs to be specified what alternative approach the FE can take.

Article 11(1)(a): Not every test scenario for a Red Team Assessment has a scope that requires a large test team. Such smaller assessments would be a suitable candidate for an internal test. Therefore, the limitations regarding the minimum size of the internal team should be lowered to a test lead and at least one additional member (total team size of two).

It is important to note that having internal penetration testers is often not affordable for small and medium-sized companies and if there are internal pentesters, it will only be limited to one or two persons. It could be that a pentester is hired to work internally from a security company. It is not clear through the text whether this person would still be seen as an internal tester.

d. Approach on cooperation

Q12. *Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.*

No

It must be stressed that the test itself is not an oversight activity. The authority leading and organising the test should be able to evaluate the results in an objective way. This relates to the provisions of Article 26/27 in level 1.

The FE should have a say in whether a host TLPT authority should be appointed as the TLTP lead and, if so, which one.

The level of cooperation should be clarified, as for example weekly status points between the TLPT authority and FE may not be feasible.

Q13. *Do you have any other comment or suggestion to make in relation to the proposed draft RTS? If so, please provide detailed justifications and alternative wording as needed.*

The TI-provider remarks in Question 9 concerning the use of existing threat intelligence services should be further clarified.

Also, the scenarios selection for testing should be further clarified. The mandatory scenarios should be relevant for the company, so it would be useful to clarify if this can be decided by the company itself. Is one scenario also possible if only confidentiality for example is the main assumed breach risk scenario?

Article 1 should include the definition of the "*red team*". The activities performed by the red team are mentioned in several instances in the RTS, but the definition is missing.

As no new entities (e.g. control team vs. white team) are introduced by the RTS compared to the TIBER framework, no new wording should be introduced either. Instead, the wording of TIBER-EU should be used wherever possible.

Explicit reference must be made to the issuance of the attestation (only mentioned for pooled tests).

Purple teaming is very valuable precisely to learn from as an organisation. It would be preferable to make it mandatory.

Timelines for all approvals that must be issued by the TLTP authority are missing throughout the RTS (e.g. Article 7(6), Article 8(3) etc.) Moreover, it is essential that the authorities' system of information used to keep the data related to TLPT performed by the FEs is secure, considering the highly sensitive nature of this information.

Article 2(3): the RTS is intended to only clarify the provisions of DORA. If DORA provides an exemption from TLPT testing, then the RTS should not allow exempt entities to be bound to perform tests.

Article 6(5): the listed criteria are complicated, and it might be difficult to determine most of them.

Article 8(7): it might be difficult in some cases to retain appropriate availability of all interested parties.