AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Second batch of policy products under the Digital Operational Resilience Act

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

In light of the European Supervisory Authorities (ESAs)' joint consultation on the second batch of Level 2 policy products under the Digital Operational Resilience Act (DORA), this paper provides concrete suggestions and amendments to strengthen the principle of proportionality and legal certainty. In order to ensure robust operational resilience for the European financial sector, the ESAs should consider refinements of the framework for subcontracting, threat-led penetration testing, major incident reporting and oversight harmonisation.

Introduction

The ESAs run a public consultation on the second batch of draft policy products under the mandate of DORA. The package includes four draft regulatory technical standards (RTS), one set of draft implementing technical standards (ITS) and two sets of guidelines (GL), which aim to ensure a consistent and harmonised legal framework in the area of digital operational resilience. However, to ensure the intended objectives, further refinements are needed as explained below.

Subcontracting

Supply chain scope and application of materiality

The proposed scope of the Regulatory Technical Standards (RTS) is expansive, aiming to ensure that financial entities are able to assess the risks associated with subcontracting along the entire information and communication technology (ICT) subcontracting chain. The setting of risk management and contractual requirements to such a broad scope of subcontractors, without the application of materiality threshold, is unworkable and does not sufficiently reflect proportionate and risk-based principles. Such an approach would add significant complexity to a financial entity (FE)'s risk management practices – with a downstream impact to a third-party service provider's risk management obligations – without commensurate benefit; it fails to target supply chain risks that have the potential to materially impact the delivery of the contracted service and would in fact detract from effective risk management strategies.

Addressing risks associated with subcontracting in a risk-based manner is the most effective way of ensuring material risks and critical vulnerabilities in the supply chain are identified and managed by financial entities and third-party service providers. A financial entities' third-party risk management program is underpinned by comprehensive, risk-based due diligence processes, robust contractual frameworks, and risk-informed oversight measures that leverage the service provider's knowledge of its subcontractors and risk environment, whilst the financial entity remains ultimately accountable for managing the risks and compliance with its own regulatory obligations. A proportionate and risk-based approach is essential for overcoming the practical challenges of assessing (and managing) every unique risk across each element of a supply chain, which can involve a vast and complex ecosystem of thousands of subcontractors. This would also align, and give effect to, the intention in the DORA legislative text for a proportionate approach to ICT third-party risk management.

Therefore, a more explicit application of materiality should be embedded in the RTS. This could be achieved, at least, by aligning the scope of subcontractors in the final draft of the Implementing Technical Standards on the Register of Information ('Register ITS') with this RTS.

In the Register ITS, 'material subcontractors' is appropriately defined as 'only those subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof, including all the subcontractors providing ICT services whose disruption would impair the security or the continuity of the service provision'. This reflects a proportionate and risk-based supply chain scope which is important not only for the purposes of the register, but it also ties to risk management. It is therefore our expectation that the subcontractor scope of the Register ITS and Subcontracting RTS will be aligned and that the definition of 'material subcontractors' will be ported into the final draft of the Subcontracting RTS such that all references to 'subcontractors' should be understood to encompass 'all subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof', ie material subcontractors. This alignment would be essential for the consistent approach to and application of the Level 1 and Level 2 third-party risk management requirements.

Direct monitoring and oversight of subcontractors

The expectation that entities 'directly' monitor and oversee subcontractors reflects a step-change in proposed due diligence practices that may not provide any meaningful risk-management benefit. It should not be a necessary measure given risk management and contractual frameworks which ensure that third-parties and their subcontractors are held to established standards, whilst the FE remains ultimately accountable for assessing the associated risks and compliance with its own regulatory obligations. This is typically achieved through the following robust risk management mechanisms:

- Financial entities implement comprehensive, risk-based due diligence processes and supplier controls to ensure the risks associated with the use of subcontractors are effectively managed and mitigated.

- Third-party service providers must seek approval or consent or provide sufficient advance notice before engaging a 'material' subcontractor. A materiality threshold is applied to this requirement so that FEs and third parties (TPs) can focus on managing only those suppliers which present a risk to the delivery of the service.

- Third-parties service providers are required to due diligence their subcontractors and to make the results of this due diligence available to the FE upon request. This obligation typically applies to any subcontractor, regardless of tier, that is 'material' to the delivery of the service. The ability to access due diligence materials is an important tool for providing visibility into a financial entity's risk posture (as it feeds into the risk assessment) and contractual flow down.

- Third-party service providers are contractually obligated to flow down their risk management and oversight obligations to the entire supply chain and, typically, audit rights are specified as needing to be flowed down to subcontractors.

- Third-party service providers are required to stand behind the performance of their subcontractors.

Direct oversight of subcontractors can be resource-intensive, diverting attention and resources from strategic risk mitigation efforts of both financial entities and third-party service providers. These parties should instead focus on implementing robust risk management frameworks that are underpinned by due diligence, contractual agreements, and risk-informed oversight measures.

The risk management framework and contractual flow down of obligations to the third-party does not equate to the delegation of a FE's accountability for managing subcontractor risk along the supply chain. Rather, it is critical to enabling strategic and effective risk mitigation practices which leverage the third-party service providers' (i) expertise and nuanced understanding of their service, the subcontractor and their control environments, and (ii) their direct contractual relationship with the subcontractor. In the absence of a direct contractual relationship, it is not practicable for a financial entity to exercise direct oversight over subcontractors.

Therefore, it needs a balanced and outcomes-based approach that allows financial entities and third-party service providers to effectively manage material supply chain risks and leverage established contractual frameworks.

Article 1

Subparagraphs 1(f) – 1(h) are not relevant considerations when assessing the risks associated with subcontractors (either at onboarding stage or upon notification of a material change) as they are not impacted by the use of the subcontractor. Rather, these considerations are linked to the inherent risk level of the FE's planned usage of the service provided by the third party provider (TPP). **Therefore, these elements should be removed** as they are already captured as part of the risk considerations set out in article 1 of the Regulatory Technical Standard specifying the policy on ICT services supporting critical or important functions.

In addition, the reference to 'the concentration risks' in article 1(i) should be clarified and specified as meaning ICT concentration risks at 'entity level' and thereby aligned with article 29 of Regulation (EU) 2022/2554.

Article 3

Article 3 requires financial entities to assess a range of factors before deciding whether an ICT service supporting critical or important functions may be subcontracted by an ICT third-party service provider.

Article 3(1)(b)

The obligation for the ICT third-party provider to involve the financial entity in the decision-making related to subcontracting is overly broad in scope and does not align with the principle of proportionality. This would be particularly challenging for ICT third-party providers that service large numbers of customers, eg public cloud providers. Additionally, ICT third-party providers are by default

best positioned to know the subcontractors they need to engage and how best to use them, while a financial entity would not necessarily have this level of expertise.

Instead of the very broad obligation, article 3 (1) (b) could require (as would reflect current best industry practices) that the ICT third-party providers inform the financial entity and grant the right to the financial entity to object to subcontracting when relevant and appropriate. This way, the financial entity would still be able to exercise appropriate control over the subcontracting, while compliance would become more pragmatic and proportionate for both parties.

Article 3(1)(c)

The expectation that a FEs should 'assess' that certain contractual clauses are replicated in the contract between a third-party and its subcontractor is inherently problematic given established legal and contractual principles that preserve confidentiality as between contracting parties. These principles limit a financial entities' rights and ability to have sight of or access the terms of the contract as a non-party. As such, not only does this requirement risk overstepping the legal boundaries set for contractual relationships, but making a financial entities' compliance with its own obligations contingent upon it assessing that certain terms have been replicated risks undermining the financial entities' own ability to fulfil its regulatory obligations.

The focus should be on ensuring that the contractual framework between the financial entity and the third-party service provider is robust and provides for the flow down of obligations and standards to material subcontractors and the replication of certain clauses in downstream agreements. This would reach the same intended outcome, whilst remaining in line with accepted contractual principles and frameworks. We therefore recommend that this requirement is removed.

Article 3(1)(f)

Article 3(1)(f) provides that financial entities must consider 'the impact of a possible failure of a subcontractor on the provision of ICT services supporting critical or important functions on the financial entity's digital operational resilience and financial soundness, including step-in rights'. The phrase 'digital operational resilience' is very broad which could cause financial entities' focus on high-risk issues to be diluted, and 'financial soundness' is undefined, meaning its interaction with DORA is unclear and financial entities may end up taking divergent approaches in the face of this uncertainty. To ensure that financial entities focus on material risks, and to increase certainty for financial entities and ICT third-party service providers in implementing article 3(1)(f), we recommend that its wording be aligned with existing DORA thresholds regarding the seriousness of failures.

Specifically, article 3(1)(f) should be amended as follows. First, replace the words 'the impact of a possible failure of a subcontractor on' with the words 'the potential of a failure of a subcontractor to materially impair' and delete the words 'on the financial entity's digital operational resilience and financial soundness'.

Article 3(2)

Finally, article 3(2) provides that financial entities should periodically re-assess whether ICT services may be subcontracted to an ICT third-party service provider. This re-assessment must reflect changes in the financial entity's business environment, including changes to the business functions, ICT threats, concentration risks, and geopolitical risks. While we encourage the periodic re-assessment of risks, the terms used in Article 3(2) are currently not aligned with similar terms used in DORA, which creates additional uncertainty and complexity for financial entities when conducting their (re)assessment. As such, we recommend that the wording in Article 3(2) be aligned with existing wording used in DORA, namely 'ICT risk' and 'ICT concentration risk'.

Concretely, we recommend the following amendments to article 3(2): replace the phrase 'ICT threats, concentration risks and geopolitical risks' with the phrase 'ICT risks that may create a material impairment to the financial entity as described in Article 3(22) of Regulation (EU) 2022/2554, ICT concentration risks and geopolitical risks'.

Article 4

Article 4 is intended to set out conditions for the provision of ICT services supporting critical or important functions (as reflected in the title of article 4 and in the recitals to the draft RTS). As such, it should be made clear that the requirements described in article 4 are scoped only to ICT services supporting critical or important functions, to avoid unnecessary cost or complexity being introduced to minor ICT services that serve no critical or important function.

Concretely, the first paragraph of article 4 should be amended as follows. First, insert after the words 'identify which ICT services support critical or important functions' the words 'describe which critical or important functions those ICT services support in sufficient detail to enable the ICT third-party service provider to identify which elements of its ICT services support critical or important functions of the financial entity'. Second, insert after the words 'the written contractual agreement shall specify' the words 'in respect of ICT services supporting a critical or important function'.

Article 4(c) requires ICT third-party service providers to assess 'all risks… associated with the location of the potential subcontractor'. This is very broad and it is not clear what risks this is intended to encompass (eg it potentially requires an ICT third-party service provider to consider risks that are entirely unrelated to any financial entity). We therefore recommend clarifying that this article refers to risks to ICT services supporting a critical or important function.

Article 4(f) requires ICT third-party service providers to ensure continuous provision of their services (as reflected in the service levels and other contractual obligations applicable to the ICT third-party service provider) even in case of failure by a subcontractor. We recommend clarifying article 4(f) by inserting a comma after the word 'subcontractor' to ensure that it is clear that the article requires the ICT third-party service provider to meet its service levels.

Article 4(g) calls for the contract to specify 'the incident response and business continuity plans in accordance with Article 11… to be met by the ICT subcontractors'. It is unclear what standard this

article is attempting to set with respect to ICT subcontractors – for example, whether they should comply with the financial entity's business continuity plan or whether they should comply with their own business continuity plan. By contrast, article 30(3)(c) DORA, which sets out the provisions to be included in contracts with ICT third-party service providers, uses the phrase 'implement and test business contingency plans and have in place ICT security measures…' – the wording is clearer and more precise than the wording of the draft RTS. To clarify this provision of the draft RTS, and to ensure consistency with the text of DORA, article 4(g) of the draft RTS should be aligned with article 30(3)(c) of DORA.

As a general remark, it is not appropriate in all cases for the written contractual agreement between the financial entity and the ICT third-party service provider to 'specify' operational details like the incident response, business continuity plans, service levels, security standards and security features to be met by subcontractors.

This requirement assumes a more traditional service model where there is a one-to-one relationship between the financial entity and the ICT third-party service provider as well as a one-to-one relationship between the primary service and the subcontracted service. This is not how subcontracting works for all ICT services today. For example, in the public cloud infrastructure service model:

- The service is one-to-many. A single subcontractor engaged by a cloud service provider (CSP) is relevant to potentially all the CSP's customers. Although the CSP will have a separate contract with each financial entity (this could be hundreds of financial entities), it will only have one contract with the subcontractor. Therefore, it is not possible for each financial entity to specify how a CSP addresses operational details like incident response, business continuity plans, service levels, security standards and security features are addressed with subcontractors.

- The CSP may subcontract components of the service. These components are building blocks of the overall service, but they don't always have a one-to-one relationship with the service provided by the CSP. Therefore, a financial entity will not be best placed to determine how to most effectively address operational details like incident response, business continuity plans, service levels, security standards and security features with subcontractors.

Instead, the primary contract should set these expectations as between the financial entity and the ICT third-party service provider and require the provider to ensure that they are addressed in the subcontract without dictating how.

We also encourage the ESAs to remove the reference to article 11 and article 28(10) in the RTS. These articles are framed as direct requirements on the financial entity and should not be entirely carried over to the subcontracting context – especially when this would result in the RTS addressing these topics vis-a-vis subcontractors in more detail than article 30 addresses them vis-a-vis the ICT third-party service provider.

Finally, we encourage the ESAs to remove the reference to termination rights 'in case provision of services fails to meet service level agreed by the financial entity'. As written, there is no materiality threshold. Therefore any failure to meet a service level could justify termination. This requirement overlaps with the requirement in DORA article 28(7)(a) which refers to termination for 'significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms'. The original Commission draft of article 28(7) only referred to 'breach'. However, during the legislative process the Parliament and the Council both agreed that mere breach was too low a threshold for termination. The RTS should not override the outcome of the legislative process on article 28(7) or unnecessarily duplicate it.

Proposed amendments:

- Article 4, c): Replace the words 'assess all risks' with the words '**assess all risks to the ICT service supporting a critical or important function that are relevant to whether there might be a material impairment of the kind described in Article 3(22) of Regulation (EU) 2022/2554**'. Replace the words 'potential **subcontractor' with the words 'current or potential subcontractor**'.
- Article 4, e): 'that the ICT third-party service provider is required to **specify in its written contractual agreement with the ICT subcontractor** the monitoring and reporting obligations of the subcontractor towards the ICT third-party service provider, and where relevant, towards the financial entity'.
- Article 4, f): insert a comma after the word 'subcontractor' to ensure that it is clear that the Article requires the ICT third-party service provider to meet its service levels.
- Article 4, g): '**that the ICT third-party service provider is required to specify in its written contractual agreement with the ICT subcontractor** the **business contingency plans described in Article 30 (3) c).** ~~**incident response and business continuity plans in accordance with Article 11 of Regulation (EU) 2022/2554**~~ and service levels to be met by the ICT subcontractors'.
- Article 4, h): '**that the ICT third-party service provider is required to specify in its written contractual agreement with the ICT subcontractor** the ICT security standards and any additional security features, where relevant, to be met by the ~~subcontractors in line with the RTS mandated by Article 28(10) of Regulation (EU) 2022/2554~~'.
- Article 4, j): 'that the financial entity has termination rights in accordance with article 7~~, or in case the provision of services fails to meet service levels agreed by the financial entity.'~~

Article 5

The expectation for the FE to monitor subcontracting chain through the review of contractual documentation between the third-party and its subcontractor introduces significant legal, commercial and operational complexity.

Firstly, it puts at risk the core tenet of confidentiality as between contracting parties and could raise conflict of law considerations, such as antitrust concerns (eg if supplier pricing arrangements are exposed to their FE clients). It also raises the possibility of an impact to the core common law legal doctrine of contractual privity, by giving an entity which is not a party to the contract between ICT

service provider and its subcontractor visibility over and a say in contract formation. This would also risk undermining the third-party's ability to negotiate suitable terms with its subcontractors.

Furthermore, it might lead to the unintended consequence of actually limiting the ability of financial entities to properly assess the risk of using a subcontractor. Given the large number of subcontractors (and their subcontractors, etc) in the chain, the risk management teams of financial entities will end up spending more time looking into the subcontracting chain, that might have not much to do with the provision of critical services, rather than fully considering the implications of using their main service providers.

As noted above, the contractual framework between the FE and third-party should provide for the cascading of obligations along the supply chain in respect of material subcontractors, including that these be specified or reflected in downstream contractual arrangements. Requiring FEs to review contractual documentation should therefore not be a necessary measure. The regulatory emphasis should therefore be on robust contractual frameworks focusing on outcomes-based measures that ensure effective risk management and regulatory compliance, thereby allowing contracting parties the flexibility to negotiate and agree contractual terms that reflect the specific circumstances and risks of the third-party and/or subcontractor engagement. Requiring financial entities to review contractual documentation, with no focus on operational resilience, is excessively burdensome for both the financial entities and ICT third-party service providers. Where financial entities wish to review documentation to address a specific point, they may exercise their audit rights pursuant to the Regulation. Accordingly, proposed article 5(2) should be deleted.

Finally, this requirement would have a significant real-world impact if it were to be operationalised – particularly if the expectation extended along the entire subcontracting chain. The sheer volume of thousands of financial services firms intervening in contractual negotiations would impose a huge administrative burden, extend negotiation timelines and potential industry-wide disruption that itself would risk the stability of the financial system.

As a related point, entities within scope of DORA continue to remain concerned about contractual remediation given the potentially enormous scope of services, noting the January 2025 implementation deadline and comments by the ESA's in response to the first batch of regulatory technical standards that there will be no transitional arrangements for contracts. Whilst we are encouraged by verbal reassurances that we could expect a pragmatic approach to be taken involving remediation upon the natural lifecycle of the contract, the risk of diverging supervisory approaches to enforcement remains a significant concern.

The lack of transitional arrangements is particularly concerning for ICT service providers given that article 4(e), (g), (h) and (i) contain provisions that providers must contractually agree to include in their own subcontractors. Although a pragmatic supervisory approach may offer comfort to financial entities, it will not protect ICT third-party service providers from contractual liability if financial entities insist on updating contracts to address subcontracting by January 2025 but - because of the lack of transitional arrangements - feel unable to allow the provider any time to update their own subcontracts.

The ESAs should align Article 5 with the approach in the IST on the Register of Information, which correctly focuses on subcontractors that effectively underpin the provision of the ICT services. If this is not clarified, financial entities would have to monitor a provider simply because it provides an ICT service to another provider in the chain regardless of whether that service is material to the ICT service that the financial entity actually consumes. In this scenario, the chain could easily run to thousands of providers.

This would be extremely disproportionate. It would create an enormous operational burden on financial entities and every provider in the chain without meaningfully improving sectoral resilience. To the contrary, it could distract financial entities from monitoring genuinely material ICT subcontractors because their resources will have to be spread across all ICT subcontractors regardless of materiality.

The Financial Stability Board (FSB) Toolkit on Third Party Risk Management (3.5.1) highlights these issues and makes the same recommendation:

- 'Addressing risks associated with service providers' supply chain in a risk-based manner is one of the most significant ongoing practical challenges for both financial institutions and service providers. Given the growing complexity and length of service providers' supply chains, particularly in areas such as ICT, it can be impractical for each financial institution to directly assess and manage every unique risk across each element of their third-party service providers' supply chains. Consequently, this section of the toolkit recognises the need to apply the principle of proportionality in the management of risks from key nth-party service providers. In particular, the toolkit acknowledges that there are practical limitations to financial institutions' ability to directly monitor and manage these risks.
- 'Focusing on those nth-party service providers that are knowingly essential to the delivery of critical services to financial institutions or which have access to confidential or sensitive data belonging to the financial institution can be more consistent with a proportionate, risk-based approach.'

Article 6

The requirements for material changes to subcontracting arrangement should be limited to ICT services supporting critical or important functions. As currently drafted, article 6 is not explicitly scoped to subcontracting arrangements for ICT services supporting critical or important functions. This should be clarified given the mandate under DORA article 30(5) is limited to subcontracting ICT services supporting critical or important functions.

Proposed amendment:

- **Article 6: '**In case of any material changes to subcontracting arrangements **for ICT services supporting critical or important functions when an ICT service supporting critical or important functions is subcontracted the financial entity shall**...'

The requirement that financial entities approve or not object to changes to subcontracting arrangements is impractical, and may be incompatible with the one-to-many nature of public cloud

services and other technology providers, which service multiple financial entities from a single infrastructure. In service this model, the real-world impact of a service provider having to await and manage approval or non-objections from numerous financial entities would not only create a substantial administrative burden, but could lead to the loss of access to key services, negatively impacting resilience and competitive capabilities. We therefore suggest this paragraph is removed, and have proposed amendments to paragraph (4) which appropriately capture the notification process while reflecting the practical limitations of such models.

Proposed amendments:

- Paragraph 1: 'In case of any material changes to subcontracting arrangements **in relation to ICT services supporting critical or important functions**, the financial entity shall ensure, through the ICT contractual arrangement with its ICT third-party service provider, that it is informed with a sufficient advance notice period to assess the impact on the risks it is or might be exposed to, in particular where such changes might affect the ability of the ICT third-party service provider to meet its obligations under the contractual agreement, and with regard to changes considering the elements listed in Article 1.'
- Paragraph 2: 'The financial entity shall inform the ICT third-party service provider of **any objections to the proposed changes** ~~its risk assessment results~~ as referred to in paragraph 1) by the end of the notice period.'
- ~~Paragraph 3: **The financial entity shall require that the ICT third-party service provider implements the material changes only after the financial entity has either approved or not objected to the changes by the end of the notice period.**~~
- Paragraph 4: '**where appropriate**, the financial entity shall ~~have a right~~ **ensure through the ICT contractual arrangement with its ICT third-party service provider that the financial entity may** to **either (a)** request modifications to the proposed subcontracting changes before their implementation **or (b) terminate the agreement** if the risk assessment referred to referred to in paragraph 1) **reasonably** concludes that the planned subcontracting or changes to subcontracting by the ICT third-party service provider exposes the financial entity to risks as specified in Article 3(1) that exceed its risk appetite.'

The ESAs' mandate under DORA article 30(5) is to prepare an RTS to further specify the elements which a financial entity needs to 'determine and assess' when subcontracting ICT services support critical or important functions.

This does not extend to prescribing further contractual provisions over and above those included in Article 30. These are not aspects that the financial entity must 'determine and assess'. Rather, they are new requirements about how the financial entity must address the risk once a determination and assessment has been made. This a strategic decision that the Level 1 text does not prescribe. The legislative bodies made a policy choice to leave it to the financial entity to consider how best to address the risk once determined, as a number of different approaches could be taken which may or may not include imposing specific contractual requirements. Therefore, it is not appropriate for the RTS to set out specific contractual terms.

This conclusion is supported by:

- The ESAs' governing regulations, which limit the ESAs powers by providing that RTS are to 'be technical', 'shall not imply strategic decisions or policy choices' / shall not 'involve policy choices' and 'their content shall be delimited by the legislative acts on which they are based.'
- The deadline for compliance. Given the deadline for the final RTS is 17 July 2024 and the DORA deadline is 17 Jan 2025 and the absence of any transitional provisions for existing arrangements, financial entities and providers would have a maximum of only 6 months to implement these contractual changes in existing contracts. This is significantly shorter than the implementation deadlines that were provided for all the current ESA GLs, which contain equivalent contractual requirements and provide 2+ year transitional terms. This could not have been the intent of DORA Article 30(5).

Threat-led penetration testing (TLPT): pooled testing

Cross-sectoral approach

Accordance with the European framework for threat intelligence-based ethical red-teaming (TIBER-EU): The cross-sectoral approach taken within the RTS is broadly welcome and aligns with the stated intention of Article 26(11) in DORA to build the RTS 'in accordance with the TIBER-EU framework'. A cross-sector approach provides the RTS with the best chance of seeking harmonisation and standardisation of TLPT processes across the European Union. However, TIBER-EU has yet to publish comprehensive guidance concerning TLPTs with both an individual financial institution and third party provider (TPP) or for pooled tests, containing multiple financial institutions or third party providers. The RTS on TLPT maintains the concept of these tests, per the Level 1 text, however, it does not provide further guidance concerning their operationalisation. Both forms of test represent significant complexity with material legal, operational and practical challenges that have yet to become established norms within the financial or technology sectors. The financial entity, who would be accountable for administering both tests, would face significant risk if they were required by a TLPT authority to do a combined or pooled test. All stages of the TLPT explained within the RTS would not be met and the expected timelines do not reflect the complexity of either test. Further guidance concerning TLPT with third parties or pooled tests is necessary before such tests could be completed in practice. However, we also do not believe it is appropriate for specific guidance to be built within the short period remaining for the finalisation of this RTS, or without industry consultation. We recommend that combined and pooled tests are not considered by TLPT authorities until comprehensive guidance is produced by TIBER-EU. Further comments concerning the complexity of tests is included within Question 10.

Quantitative criteria and thresholds in article 2(1) to identify financial entities required to perform TLPT

The combination of the efforts needed to undertake TLPT and the scarcity of highly skilled and relevant personnel emphasises the importance of mandating TLPT solely on entities with a certain degree of systemic importance and sufficient ICT maturity. Any other approach could lead to an unduly heavy compliance burden being placed on smaller financial entities that do not have the necessary resources or skilled ICT personnel required to make a TLPT effective and useful for the purposes of protecting critical or important functions.

Further criteria relating to 'impact and systemic related factors' and ICT maturity related factors need to be considered appropriately to ensure that smaller, less ICT mature entities are not artificially

subject to TLPT requirements. To give effect to this, we propose making the following amendments to Article 2(3):

- 'TLPT authorities shall assess whether any financial entities other than those referred to in paragraph 1 shall be required to perform TLPT, on the basis of all of the following criteria. **These criteria are listed in order of their relative bearing on a TLPT authority's decision on whether the financial entity should be required to perform TLPT.**'

Approach for financial entities to assess the risks stemming from the conduct of testing by means of TLPT

AmCham Eu does not agreed with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT. The procedures for execution – specifically, the requirement to provide leg-up assistance – create risks to security for other customers because of their open-ended nature.

Article 8 of the draft RTS sets out the process for the red team testing phase of the TLPT. To expedite the red team's testing, article 8(8) enables the control team (whose members may include ICT third-party service providers) to provide 'leg-ups' to the red team, in accordance with the red-team test plan.

TLPT is an important cyber defence measure for financial entities, and 'leg-ups' can help to expedite the testing process and discover vulnerabilities in a financial entity's systems that would otherwise not be discovered. However, carrying out TLPT creates inherent risks, including confidentiality and availability risks (as the draft RTS acknowledges – see paragraph 34). These risks can be particularly acute for cloud service providers who provide services to multiple financial entities. Specifically, risks introduced by one customer carrying out TPLT could, in certain circumstances, affect many other customers, including other financial entities and, further, other non-financial institutions (including public sector organisations such as the European Supervisory Authorities and other regulatory bodies).

While we support the concept of financial entities providing leg-ups for the systems they themselves control, cloud service providers (CSPs) cannot provide leg-ups that would involve a financial entity's red team receiving privileged access to CSP's internal infrastructure that is used to serve many customers (including many financial entities). Providing any financial entity with privileged 'leg-up' access to CSP's infrastructure would introduce an unacceptable security risk to CSP and its other customers, breach CSP's confidentiality obligations to customers using that infrastructure, and may cause CSP and other financial entities and non-financial entities (including regulatory bodies such as the European Supervisory Authorities) to breach their own regulatory and confidentiality obligations to ensure the security of their systems. In other words, TLPT generally and 'leg ups' specifically should be limited to security within the cloud, not security of the cloud.

Our position is consistent with both DORA and elements of the draft TLPT RTS. We welcome that Recital 18 of the draft TLPT RTS acknowledges that 'leg ups' should be given only by the 'financial entity', to its 'ICT system or internal network', not by ICT third-party service providers. Nonetheless, to ensure clarity in the scope of the 'leg up' regime, the ESAs should clarify in Recital 18 of the RTS that TPLT does not require testers to seek, and does not require ICT third-party service providers to grant, access that could bypass controls in the relevant service and undermine the security of their infrastructure. Consequently, we recommend that recital 18 be amended as follows:

- Before the words 'ICT system or internal network' insert the words '**the financial entity's own**', and
- At the end of recital 18, add the words '**A leg up**' shall be limited to the financial entity's own ICT systems or internal networks and shall not include access to a third party ICT provider's ICT system or internal network beyond such access as the financial entity itself ordinarily has access to and undertakes for the purpose of operating the relevant critical or important function. In particular, a 'leg up' shall not enable the testers to access any third party ICT provider's ICT systems or internal networks used to support customers other than the financial entity, or that otherwise increases the risk of an adverse impact on the quality or security of the services provided to those customers'.

Proposed requirements for pooled testing

DORA Article 26(4) allows for 'pooled testing' of third party ICT service providers where testing is 'reasonably expected to have an adverse impact on the quality or security of services delivered by the ICT third-party service provider… or on the confidentiality of the data'. We welcome the inclusion of the pooled testing regime in DORA, which, in theory, can avoid unnecessary duplication of the costs and risks associated with TLPT.

However, in our view DORA's requirement for pooled testing lacks detail and faces significant practical challenges for financial entities, regulators and TPPs. The majority of the issues listed below hold true in both a pooled and a TLPT involving a single FE and a TPP. As a result, DORA could potentially lead to a situation where large TPPs with hundreds of FE clients are required to engage in TLPTs on an ongoing basis. DORA permits selected FEs to conduct TLPTs once every three years. In contrast, TPPs that support CIFs are required to 'participate and fully co-operate' whenever the FE determines they are in scope and could therefore be required to support a multitude of TLPTs in any given year. Such an outcome would be impractical. More generally, any outcome where TPPs are overwhelmed by TLPT requirements would heighten IT security, operational and legal risks for them and by extension the FEs and the financial industry as a whole. In practice, we consider annual TLPT exercises a viable maximum for TPPs.

Conversely, an FE may have several TPPs supporting its CIFs resulting in a situation in which multiple TPPs are in the scope of its TLPT. This would require bespoke contract negotiation with each TPP, it would also require their involvement in the test to some degree increasing the difficulty managing the test and risk of exposure of sensitive information of the FE.

The current draft RTS does not provide sufficient guidance to financial entities or TPPs on when to use pooled testing or how such arrangement should be put in place according to the timelines and other expectations of the current RTS.

One solution would be to recommend that pooled or tests that involve an FE and TPP are not considered until TIBER-EU publishes guidance on how to practically conduct these types of test, both pooled and any TLPT involving a FE's TPP. We wish to note that other regulators have consulted on the inclusion of third-party providers within TLPT testing and ultimately decided against it owing to the significant legal, and security complications that are created. This is largely because neither pooled testing or the inclusion of TPPs are common practice across the financial sector and significant uncertainty remains concerning any attempts that have been made by TPPs to run such tests thus far. As financial entities are ultimately accountable for tests under the TLPT RTS, the RTS does not provide

sufficient certainty to allow entities to comply with the broad TLPT requirements set out within the RTS whilst also involving TPPs within their scope.

In addition, Article 8(10) allows the TLPT to be suspended where continuing the test risks 'impact on data, damage to assets, and disruption to… the financial entity itself, its counterparts or to the financial sectors'. As TLPT may affect third-party ICT providers too – and as described in our response to Question 6, damage to these providers can have more wide-ranging consequences than damage to individual financial entities – this Article should be amended to include third-party ICT providers. Though the inclusion of TPPs in the scope of an FE's TLPT should be avoided until further guidance is produced.

To address this, we recommend that the ESAs insert a new Article 8(10a): **'Under circumstances triggering risks of impact on quality or security of services delivered by an ICT third-party service provider, the control team lead must suspend the TLPT insofar as it triggers those risks and consider continuing the TLPT using a pooled testing exercise as described in Article 26(4) of Regulation (EU) 2022/2554'.**

Preparation phase

TPPs supporting CIFs

TLPTs are predicated on targeting the 'critical and important functions (CIFs)' that a financial entity offers in specific jurisdictions and the ICT systems that support those CIFs. The TLPT RTS uses the concept of TPPs who 'support' CIFs, without any materiality threshold. Financial entities use a significant array of TPPs to support CIFs. This could result in a impractically larger number of TPPs being included in the scope of the TLPT. Ensuring sufficient legal rights, confidentiality of sensitive information and security controls for such a broad test would not be feasible. As such, we recommend that some form of materiality threshold is included within the RTS in order to clarify how far a TPP has to 'support' a CIF in order to qualify as a TPP that needs to assist a financial entity with its TLPT with respect to that CIF.

Contractual challenges

In addition, financial entities utilise TPPs that vary in size, complexity and the services they offer. While the discussion has focused on CSPs and some other large technology companies, many TPPs will simply not have the technical resources to 'participate and fully cooperate' in TLPT from all of their financial services clients as required by DORA Art. 30(3.d).

Further, we anticipate that securing the contractual rights required in article 30(3.d) will be difficult to achieve as it amounts to a carte blanche right that could later violate the security policies of the TPP. It is worth considering that the TLPT's scenario(s) and specifics of the TLPT test will not have been determined in prior negotiations nor specified within any existing contract between the FE and TPP. Any red team plan that includes scenarios with a TPP would require separate contractual negotiations (including non-disclosure agreements (NDAs)) and planning between the financial entity and the TPP. This would have to be undertaken during the preparation phase and would add a significant level of uncertainty regarding the timing and legal feasibility of the TLPT. This would be further exacerbated if the TLPT authority rejects or requests changes to the TLPT scoping document as per RTS article 6(9). In such a case, the FE may then need to renegotiate and amend legal terms with the TPP to achieve the changes. The FE would also need to discuss changes with the testers and TI providers which could impact the contract between the FE and those providers. Should either the providers or the TPP

object, the FE will be required to seek approval for changes from the TLPT authority. Conceivably, this circular series of approvals and contractual negotiations could continue for multiple rounds and ultimately result in extended delay and uncertainty to the TLPT.

Accountability and risk assessment

The financial entity in the RTS is responsible for all risk management of a TLPT and is required to conduct a full risk assessment. The inclusion of TPPs in a TLPT, or a pooled test scenario, create uncertainties about how liability and risk management should operate in practice. Additionally, there is a risk of uncertainty arising the assignment of different roles and responsibilities within the control team, given that the RTS includes TPPs automatically as participants within the control team. As a general principle, we think that ICT third-party service providers should only be involved where a TLPT needs to assess a CIF that is supported by that specific ICT third-party service provider. This means that the definition of the control team needs to accommodate some flexibility to accommodate for scenarios where an ICT third-party service provider must be included – e.g. due to its support of critical or important functions (CIFs) of the financial entity – and where such involvement is not necessary because the FE does not rely on that service provider to support a CIF. However, even with this change, there will remain significant practical challenges to operationalising a TLPT including TPPs.

Choice of TI providers and testers

The preparation phase requires FEs to ensure that threat intelligence providers and external testers are compliant with Article 5(2) and have sufficient experience and expertise to undertake a TLPT. There is insufficient experience of shared or pooled tests within the external market and financial entities would be unlikely to source any individual with the required technical knowledge in 5(2)(e)(ii) and 5(2)(f)(ii). Further, it is unclear how to proceed if the FE and the TPP have conflicting views regarding the suitability of the testers or TI providers. This would be compounded in the case that multiple TPPs were in scope of the FE's TLPT or in the case of a pooled test where multiple FEs may not accept decisions made various control groups.

Scenarios and TIP report

Annex III does not make clear whether the TI provider would be expected to apply paragraph 2 to any in-scope TPPs as well as the financial entity. Doing so would represent a material extension of the TIP work and would likely require renegotiation of the TIP contract. This is another area where there is a risk of a circular series of approvals and changes between the FE, TIP/testers, TPP and the TLPT authority in a pooled test or TLPT with TPPs in scope.

Testing phase

Approvals from the TLPT authority

As per our comments above, the RTS creates a number of instances where the TLPT authority is required to issue a validation or approval before the FE can progress in the TLPT. In a pooled scenario, we are concerned about the potential for extended delay while multiple TLPT authorities from the participating FEs consider different requests or information submissions from the control teams. As these approvals are required during the testing phase and involve fundamental elements of the test such as leg ups or actions to maintain confidentiality, delays could result in breaches to the terms of the test or considerably delay progression of the TLPT.

Control team

There is significant uncertainly about how a control team would manage a test in a pooled test or in a TLPT with multiple TPPs in scope. In either scenario, all firms involved may reasonably expect to be included in the control team. This could result in the control team becoming unmanageable in size and impact the ability for quick decision making or frequent contact with the TLPT authority. It is also likely that participating firms would seek to restrict sensitive information from other participants out of concern for security and competition law. At a minimum, NDAs would be required across all participating firms which would create a web of legal agreements that would be difficult to manage and contribute to a material extension of the proposed timelines. For these reasons, per the comments above with respect to pooled testing generally, it is critical that TLPT authorities consult and gauge the views of TPPs before binding guidance around pooled testing is brought in.

Closure phase

Mandatory purple teaming/ closure phase

The closure phase process for the TLPT RTS is unclear in the context of a pooled test. Mandatory purple teaming, for instance, does not make practical sense within a pooled test as it would theoretically entail a variety of financial entities and their respective blue teams working individually, or grouped, with the third party provider. The remediation plan, in addition, is unclear and it is unknown how it could interact with the identified financial entity, other financial entities and the third party provider. Remediation would also likely need to be undertaken alongside the third party provider and therefore would be more complex to resolve. The third party provider, in addition, would likely be working alongside the other financial entities who will all have separate controls and will have other services hosted on the third party. Commercial relationships with third party providers are complicated as they relate to sensitive or proprietary technology which have long implementation timelines if changes are required. It is equally unclear if the identified financial entity could be liable for ensuring the third party provider implements remediation changes given their accountability for all aspects of the TLPT.

TPPs are also concerned about any potential outcome where the results of TLPTs are disseminated to a large number of FEs. In order to effectively manage the operational, security and legal risks inherent in the TLPT, the TPP would need to restrict access to the full results so as to ensure that the audience for these sensitive security details is strictly limited. It poses a high security risk to both the TPPs and the industry at large to make these vulnerabilities available to all the FEs potentially involved in the pooled TLPT.

One method for addressing this risk might be to create a secure repository for TLPT results where access could be controlled, though this would come with significant security challenges that would need to be addressed.

At the same time, it is unclear how that could be achieved while also still allowing the FEs, in particular any FE designated as the lead FE that is tasked with ‘directing’ the TLPT, to comply with its regulatory requirements seeing as there is nothing in either the Level 1 text or the RTS which would relieve them of responsibility for completing the full scope of their TLPT. Without clarity on how the TPP will be able to adequately protect sensitive data while still allowing the FE’s to comply with their wider requirements in the RTS, it will be difficult or impossible to conduct a pooled TLPT.

Additional comments on the proposed draft RTS

Involvement of service providers in TLPT

The draft RTS provides little information on the involvement of TPPs in the TLPT process, beyond acknowledging in article 1(1) that the 'control team' may include TPPs. As the TIBER-EU framework white team guidance describes (in section 4.1), ICT TPP personnel often have detailed knowledge about that provider's systems and about how the financial entity uses those systems, and therefore can make valuable contributions to the testing process. For this reason, the TIBER-EU framework white team guidance encourages the control team to engage in discussion with third party ICT service providers 'at an early stage' to discuss the TLPT, and considers that 'a small number of staff from the third-party provider(s) can join the White Team'. We agree with the TIBER-EU white team guidance that third-party ICT service providers should be informed of and have the opportunity to input into TLPT exercises.

To ensure that the draft RTS is aligned with the TIBER-EU guidance in this respect, we recommend clarifying that, where an ICT third party service provider is impacted by the TLPT process, that ICT third party service provider should always be informed about the TLPT and, where relevant, be given the option to participate in the testing. This will improve the quality of TLPT and ensure the draft RTS is aligned with the TIBER-EU framework.

To address this, we recommend that the ESAs insert the following text at the end of article 6(4):

- **'To the extent the scope specification document envisages that an ICT third-party service provider will be within the scope of, or otherwise affected by, the TLPT, that third party ICT service provider shall be made aware of and, as appropriate, given the opportunity to participate in, the control team.'**

However, while this is necessary from a risk management perspective, for the FE, which may have multiple TPPs supporting CIFs, this will create potentially unmanageable complexity, or a control team that is too large to be practicable. In a pooled test, it is also unclear whether the TPP would be expected to participate in the control team of every FE in the test, or whether every FE in the test would be expected to sit on a control team run by the TPP. In either case, such arrangements would necessitate a complex web of legal agreements which will be dependent on approvals from TLPT authority(ies) and would likely have severe impacts on the feasibility of the timelines set out in the RTS. It is therefore another reason why the inclusion of TPPs in an FEs TLPT, or pooled testing, should be avoided until such time as TIBER guidance is produced.

Notification of vulnerabilities to service providers

Article 9(3) of the draft RTS requires test reports to be given to the control team and test managers, and article 8(10) sets out obligations of the red team in relation to vulnerabilities they discover during their testing that may trigger risks of 'impact on data, damage to assets, and disruption to critical or important functions'. However, neither Article sets out an obligation to notify ICT third-party service providers of these test reports or vulnerabilities, to the extent those reports or vulnerabilities relate to the ICT third-party service provider, nor expressly addresses situations where a vulnerability in an ICT third-party service provider may affect multiple financial entities.

Notifying an ICT third-party service provider of vulnerabilities in its service of which it would otherwise not be aware (as the ICT third-party service provider may not be participating in or aware of the TLPT)

reflects best-practice vulnerability disclosure practices, and enables the ICT third-party service provider to identify and address vulnerabilities that may affect multiple customers. In turn, this improves security for all customers of the ICT third-party service provider, including other financial entities. This is the case even where the financial entity in question is able to work around or mitigate the security risks presented by the vulnerability, as other financial entities may not be aware or have taken the same mitigation measures.

To address this issue, and encourage best-practice vulnerability sharing during the TLPT process, we recommend the following amendments to the draft RTS:

- Insert, at the end of article 9(3), the words '**and, to the extent the report contains information directly relating to any vulnerability in the service of an ICT third-party service provider, the control team shall also provide the relevant sections, appropriately redacted, of the red team test report to the ICT third-party service provider as are necessary for that provider to assess and remediate the vulnerability.**'
- Insert new article 8(12): '**At any time during the active red team testing phase, upon discovery of a vulnerability in the service of an ICT third-party service provider that could adversely affect the delivery or security of services that provider provides to the financial entity or other customers, the testers will immediately inform the ICT third-party service provider of that vulnerability, and provide all relevant information they have learned about the vulnerability to the ICT third-party service provider. The testers shall provide such information to the ICT third-party service provider in a commonly-used machine-readable format and, where possible, through the ICT third-party service provider's vulnerability management system**'.

Confidentiality

Sharing information relating to the security of ICT systems throughout the TLPT process is consistent with best-practice testing practice and article 26(3) of DORA, which calls for participation in the TLPT process by ICT third-party service providers where necessary.

However, information relating to the security of ICT systems is, by its nature, highly sensitive. Article 4 of the draft RTS requires that information about the TLPT process be treated confidentially and on a 'need-to-know' basis within a financial entity. However, the RTS does not oblige entities involved in the TLPT process to ensure the confidentiality of such information when it is shared between different entities involved in the TLPT process. To encourage the sharing of relevant information between those entities, including ICT third-party service providers, the Regulation should include an explicit requirement to treat that information securely and confidentially. FEs should also be obliged to achieve explicit commitments from the TPPs to act in a similar manner.

We propose to insert new article 4(2)(g) as follows:

- **'Financial entities shall establish technical, legal and organisational and measures ensuring that any information shared between parties in connection with the TLPT, including between the financial entity and the ICT third-party provider, is protected from unauthorised access, and is used and disclosed only for the purposes described in this Regulation.'**

Major incidents reporting

The DORA incident reporting regime constitutes the most comprehensive reporting regime for any equivalent regulatory jurisdiction. The timelines for reporting, alongside the level of detail required across all classification criteria, will require substantive uplift across financial entities and could detract entities from concentrating on incident management.

While financial entities recognise that the ESAs have sought to provide proportionality to the regime via including an encompassing 'critical services affected' classification, the additional definition has resulted in no materiality being provided. The original consultation by the ESAs noted that, without a high materiality threshold, PSD2 indicated that there would be 'significant overreporting' of incidents that did not have a high adverse impact. Article 6(b) defines critical services as any services which is 'supervised by competent authorities.' AmCham EU's assessment suggests this would include any service or function in the financial entity and therefore de-facto removing any materiality threshold.

To reduce the level of burden being placed on financial entities, the ESAs should reconsider the level of information they expect from entities within the initial and intermediate reports. The 72 hour period for both reports constitute the primary hours by which a financial entity will be responding and recovering from an incident and any detailed reporting will serve to detract an entity from incident risk management. DORA's reporting is predicated on PSD2 data fields, which does not reflect the greater level of complexity entities face from incidents that are not payments-related. Payments incidents immediately inform entities concerning a variety of criteria, such as transactions, clients affected, geographic location and economic impact. This information is more diffuse and difficult to estimate for an ICT-related incident or application. Detailed criteria should therefore be predominantly required within the final report and/or 'yes, if applicable' in the majority of circumstances.

The proportionality applied to financial entities for incident reporting is to allow microenterprises and non-significant financial entities to not report during weekends or bank holidays. This should be expanded to significant financial entities for intermediate or final reports. Incidents are often insignificant, as stated in prior ESA consultations, and it is unclear what utility is provided by reporting on intermediate and final reports within these time periods. Incident management teams are critical during the first 24 hours of response and recovery, however, the information provided within incident reporting during the intermediate and final stages are often tangential to the incident itself. Highly impactful or severe incidents during a weekend of bank holiday will always be subject to considerable supervisory oversight for significant entities and it is unclear how the competent authority would use intermediate or final reports during weekends or bank holidays. Expansion of proportionality for significant institutions would allow entities to continue to report incidents at the initial stage while recognising that any significant incident will face supervisory attention through a weekend or bank holiday nonetheless.

AmCham EU expresses significant concerns with the recurring incident requirements in DORA. It is unclear regarding what root cause information a financial entity should use for recurring incidents. If a financial entity is forced to utilise the criteria within data field 4.1, the recurring requirements would

force significant overreporting of incidents. The criteria included remains high-level given the diversity of incident root causes and the multifaceted nature of ICT systems and applications. Initial analysis confirmed that, through 2023, financial entities would overreport significantly in relation to the change management and software compatibility criteria despite limited correlations between the specific root causes that underpinned those incidents. As the recurring incident requirement is based on demonstrating where a financial entity could have deficient risk management controls, number 4.3 should be used for recurring incidents where the entity has determined clearly that two incidents are related. Further clarity concerning the reporting of recurring (for instance if consolidated or through the normal process) would be welcome. AmCham EU proposes the following amendments:

- Data field 4.1 Root causes of the incident; Instructions: 'The following categories shall be considered **unless being reported as a reoccurring incident**'
- Data field 4.3 Information about the root causes of the incident; Description: 'Description of the sequence of the events that led to the incident **and description of root cause similarity when being reported as a recurring incident**.'
- Data field 4.3 Information about the root causes of the incident; Instructions: 'Description of the sequence of events that led to the incident including a concise description of all underlying reasons and primary factors that contributed to the occurrence of the incidents. **Include description of how the incident has a similar apparent root cause if the incident is classified as a recurring incident. The data field is mandatory if the incident is classified as a recurring incident.**'

The incident template RTS should be aligned further with the incident classification RTS in certain areas. The classification criteria clarified that all economic cost criteria would 'not include costs that are necessary to run the business as usual' which is further included in the Guidelines on aggregated cost and losses. This phrasing should be further emphasised within the recitals and specific data fields relating to economic costs. Including cost information that is within usual business costs would result in material overreporting, especially in relation to staff costs for the length of incident reporting. For instance:

- NEW (5): '**The economic impact of the incident shall be based on Article 7 of the proposed RTS under Article 18(3) DORA and only include costs and losses that exceed the business-as-usual costs.**'
- Data field 4.17 staff costs: 'amount of staff costs **that exceed business-as-usual costs**, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff.'

The reporting templates include a number of data fields which would require the financial entity to report confidential contractual information concerning their clients and the financial entity. These data fields should be removed as the fields would likely result in the financial entity reporting high-level information-only. Data fields 4.4, 4.5 and 4.18 all relate to confidential information concerning contracts, non-compliance and regulatory breaches where a financial entity would be uncomfortable providing detailed information within reporting. Contractual costs, in addition, are not known within 20-days and are dependent on the service offered and specific contractual arrangements with an

individual client. It is unclear how all data fields relate to incident risk management and how an incident has been resolved.

Oversight harmonisation

Chapter 2, Article 3

The requested information includes sensitive details about the ICT third-party service provider's operations, security frameworks, financial entities and employee training and security awareness programmes. Ensuring the secure handling and transmission of this sensitive data presents a significant challenge, requiring robust data protection measures.

In the interest of proportionality, the authority of the lead overseer (LO) under article 3 to request information about the CTPP's subcontracting arrangements should be limited to arrangements that effectively underpin ICT services supporting critical or important functions or a material part thereof

The following draft subsections each require clarification and amendment to align them with the Regulation and other Level 2 obligations: 3(2)(a)(ii), 3(2)(d), 3(2)(i), 3(2)(l), 3(2)(p), 3(2)(q), and 3(2)(v).

Proposed articles 3(2)(p) and (q) will cause confusion as 'extractions from the monitoring and scanning systems' and 'extractions from any production, pre-production and test system or application' are undefined. As presently drafted, proposed articles 3(2)(p) and (q) would require CTPPs to produce information that would be extremely sensitive and contain information unrelated to the provision of services to financial entities. To ensure the Lead Overseer is provided with helpful information, we propose that the Lead Overseer be provided instead with summary information from these systems and applications as they relate to how services are provided to financial entities. Summary information will provide the Lead Overseer with information about the how the CTPP's monitoring and scanning systems function, while being appropriately tailored and focused on proportionality in accordance with Recital 105 of the Regulation. We propose that proposed articles 3(2)(p) and (q) be amended as follows:

- Article 3(2)(p): '**A summary description of the** monitoring and scanning systems of the critical ICT third-party service provider and of its subcontractors **that effectively underpin ICT services supporting critical or important functions or a material part thereof**, covering but not limited to network monitoring, server monitoring, application monitoring, security monitoring, vulnerability scanning, log management, performance monitoring, and incident management.'
- Article 3(2)(q): '**A summary description of** any production, pre-production and test system or application used by the critical ICT third-party service provider and its subcontractors **that effectively underpin ICT services supporting critical or important functions or a material part thereof** to provide services to financial entities in the Union.'

Subcontracting

Draft subsection 3(2)(a)(ii) causes confusion as: (i) 'entire technological value chain' is undefined within the Regulation; and (ii) the present drafting can encompass immaterial subcontractors or

subcontractors unrelated to the services provided to financial entities. Providing information regarding irrelevant subcontractors that do not effectively underpin ICT services supporting critical or important functions or a material part thereof of the CTPP nor provide services to financial entities leads to the strange outcome of CTPPs having greater responsibility for disclosure about their subcontractors than financial entities themselves.

We propose that draft subsection 3(2)(a)(ii) should align with the Final Report on Draft Implementing Technical Standards under Article 28(9) of Regulation (EU) 2022/2554 published on 17 January 2024. This would provide the Lead Overseer with the most relevant information, while also being proportionate to the risk subcontractors may pose to financial entities operational resilience.

Accordingly, we propose the following amendment to draft subsection 3(2)(a)(ii) to provide clarity and focus the information obtained on subcontractors that are most relevant to the operational resilience of financial entities.

- Subsection 3(2)(a)(ii): '[T]he critical ICT third-party provider and **its subcontractors that effectively underpin ICT services supporting critical or important functions or a material part thereof**.'

We also propose to strike the phrase 'technological value chain' and replace it with 'ICT service supply chain' as used in the Final Report on Draft Implementing Technical Standards under Article 28(9) to provide improved definitional consistency and clarity.

Inapplicability and scope

Proposed articles 3(2)(d) and 3(2)(v) should be removed and proposed article 3(2)(l) should be amended as these articles contain requests for information that a CTPP does not have. Proposed article 3(2)(i) should also be amended as it includes data centres outside the scope of the Regulation.

Proposed article 3(2)(d) should be struck as the CTPP will not have access to information such that it can provide information about market share with any degree of accuracy. As the supervisory authorities, the Lead Overseer and the ESAs will have access to the information from its supervisory activities necessary to determine the market and market share as needed.

Similarly, proposed article 3(2)(l) should also be amended as information of major incidents with direct or indirect impact on financial entities within the Union is not information that a CTPP will have at its disposal. Financial entities within the Union, pursuant to the Regulation are required to report incidents to the ESAs rather than their ICT third-party service providers. There is no obligation for a financial entity to report such incidents to their ICT third-party service providers. It is unreasonable to expect a CTPP to provide information that is contingent upon being first informed by a financial entity. Instead, we propose that the ESAs approach a CTPP if they receive an incident notification from financial entities and require more information. The following should be removed from proposed Article 3(2)(l):

- '**Information shall also include list and description of major incidents with direct or indirect impact on finanical entities within the union, including relevant details to determine the significance of the incident on financial entities and assess possible cross-broader impacts**.'

Proposed article 3(2)(v) should be removed as: (i) it is inappropriate for CTPPs for whom security is an essential part of the service they provide; and (ii) a security budget is not a relevant proxy to identify whether security is appropriate or effective in regards to a CTPP's risk management.

A security budget is not an adequate proxy to assess whether a CTPP has in place comprehensive, sound, and effective rules, procedures, and mechanisms to manage risk in accordance with Article 33(2) of the Regulation. It is unclear how a security budget provides the Lead Overseer a means to assess effective ICT risk management pursuant to Article 33(3) DORA. The most appropriate metric to assess whether an ICT has effective risk management is the security of its services.

Proposed article 3(2)(i) should be amended as it presently will include data centres that are out of scope of the Regulation. We propose the following amendment:

- 'Information about the location of the data centres and ICT production centres, including **as applicable**, relevant premises and facilities of the critical ICT third-party service provider, including outside of the Union.'

Chapter 3, article 7

Involvement of competent authorities (CAs) under Directive (EU) 2022/2555: The involvement of CAs designated or established under Directive (EU) 2022/2555 is mentioned, but further clarification on the specific roles, responsibilities, and circumstances under which their views are considered would enhance understanding.

Chapter 4

Proposed Article 4 suggests that remediation is always required pursuant to Article 35(1)(c) Regulation (EU) 2022/2554, which is not the case. Article 35(1)(c) of the Regulation indicates that the Lead Overseer does not always require remediation and that a CTPP is not compelled to remediate. To align draft article 4 with article 35(1)(c) of the Regulation, we propose the following amendment:

- 'In accordance with Article 35(1)(c) of Regulation (EU) 2022/2554 and as part of the notification to the Lead Overseer of its intention to comply **or otherwise** with the recommendations pursuant to Article 42(1)of that Regulation, **and if required by the recommendations**, the critical ICT third-party service provider shall provide to the Lead Overseer a remediation plan outlining the actions OR remedies that the critical ICT third-party service provider plans to implement in order to mitigate the risks identified in the recommendations.'

Chapter 5 – secure channels

Information provided could: (i) expose critical CTPPs and their customers both subject and not subject to Regulation (EU) 2022/2554 to significant risk; and (ii) have significant spillover effects, if the

channel's security is breached. It is important to consider the baseline security measures of the secure electronic channel.

It is necessary to have additional information regarding the definition of a secure electronic channel, including: (i) what technical information security measures the channel owner must implement to guarantee the confidentiality of data against unauthorised third-parties; and (ii) whether parties will have an opportunity to assess the security of the agreed upon secure channel.

In addition, security requirements should be extended to both the STORAGE and transmission of information disclosed. Security of information as it is initially exchanged or transmitted is not the only factor that needs to be considered in developing a secure channel. Storage of this information after it is transmitted also needs to be considered. We propose the following amendment to proposed Article 5(1):

The information CTPPs disclose will be aligned with in Articles 45 and 55 DORA, as well as the general professional secrecy obligations for EU-authorities and the general professional secrecy obligations pertaining to the specific ESA. The information that CTPPs disclose via the proposed secure channel may be sensitive in nature such that inadvertent disclosure or unauthorised access by third-parties could have negative impacts for the CTPP and its customers both subject and not subject to Regulation (EU) 2022/2554. Reiterating that the principles of professional secrecy apply to any information disclosed to the Lead Overseer via secure channel would help ensure that the information CTPPs disclosed was handled appropriately in consideration of its sensitive nature.

- Article 5(4): **'Information submitted, disclosed or reported to the Lead Overseer by the critical ICT third-party service provider shall: (a) be exchanged, handled, stored, and transmitted in accordance with the lead overseer's secrecy obligations under this regulation and the lead overseer's governing rules of procedure; (b) exchanged, handled, stored, and transmitted in a manner that protects the potentially sensitive nature of the information shared.'**
- 'The critical ICT third-party service provider shall provide the requested information to the Lead Overseer through the secure electronic channels indicated by the Lead Overseer in its request. **The secure electronic channel must present technical information security measures to guarantee the confidentiality of data against unauthorised third-parties, certified in accordance with international best practices and standards for security and encryption**.'

Chapter 6

The information the Lead Overseer requests regarding subcontracting arrangements is overly broad and not appropriately tailored to how ICT third-party service providers provision services. The standard should limit the information disclosed regarding subcontracting to those entities that effectively underpin ICT services supporting critical or important functions or a material part thereof.

- We propose the following amendment to proposed article 6: 'A critical ICT third-party service provider which is required to share information on subcontracting arrangements which effectively underpin ICT services supporting critical or important functions or a material part

thereof shall provide the information according to the structure and the template set out in Annex I of this Regulation.'

The information requested in the template for sharing information on subcontracting arrangements is not tailored to the types of subcontractors CTPPs employ and how CTPPs provision services. In our view, the 'General Information' and 'Overview of Subcontracting Arrangements' fields require amendment. Specifically, the request for information regarding: (i) mapping of subcontracting arrangements; and (ii) the description of the types of ICT services provided to Financial Entities in the 'Overview of Subcontracting Arrangements' field does not reflect how CTPPs provision cloud services to customers. CTPPs will not have insight into how customers are using their services.

- We propose that 'mapping of the subcontracting arrangements, including a short description of the purpose and scope of the subcontracting relationships (including an indication of the level of criticality or importance of the subcontracting arrangement for the CTPP)' be amended to '**a short description of the purpose and scope of the subcontracting arrangement**'. We also propose that 'Specification and description of the types of ICT services subcontracted and their significance to the ICT services provided to financial entities' be struck.

Chapter 7

To further prevent intra-EU fragmentation and potential market disruption, we propose that draft Article 7 include provisions that ensure the Lead Overseer and the Oversight Forum can prevent unilateral decisions that could disrupt operations of financial entities beyond a Member States. We propose the following amendment:

- Article 7(2)(3): **'Whether its assessment could disrupt the operations of the financial entities in the union.'**
- Article 7(2)(5): '**Reflecting a risk-based approach and the principle of proportionality, the lead overseer shall work with the competent authority to ensure that the competent authority does not take any unilateral decisions that could disrupt the operations of the financial entities in the union beyond the member state.'**

Conclusion

The ESAs' joint consultation regarding the second batch of Level 2 policy measures under DORA is a step in the direction towards a successful implementation of DORA, and it provides the opportunity to fine-tune practical aspects of the framework before the adoption of the European Commission's delegated acts. To ensure robust digital operational resilience while providing workable solutions for the European financial sector, the above-mentioned refinements for subcontracting, threat-led penetration testing, major incident reporting and oversight harmonisation are needed.