FIA.org

FIA Feedback on DORA RTS on TLPT

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

Accordance with TIBER-EU: The financial sector supported the stated intention of Article 26(11) in DORA to build the RTS "in accordance with the TIBER-EU framework," however, TIBER-EU has yet to publish comprehensive guidance concerning TLPTs with an individual financial institution and third-party provider or 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, does not provide further guidance concerning their operationalisation. **We do not believe it is appropriate for specific guidance to be built within a short period, without industry consultation or prior TIBER-EU guidance, concerning TLPT with third parties or pooled tests.** 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 enforced 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 all timelines do not represent the complexity of either test. **We recommend that combined and pooled tests are not considered by TLPT authorities until comprehensive guidance is produced by TIBER-EU.** Further guidance concerning the complexity of tests is included within Question 10.

Enforced purple teaming:
The RTS introduces mandatory purple teaming which is beyond the parameters of TIBER-EU and not a stated requirement within DORA Level 1 text. While we recognise the argument for purple teaming, in that it can generate "a significant amount of learning for the institution involved," this is generally only experienced by financial institutions who demonstrate multiple vulnerabilities within their red teaming exercise. For mature financial institutions, who often have their own internal testing programs, red team exercises by external parties may yield limited vulnerabilities or learnings which is expected when faced with a highly adept technological infrastructure and control environment. A mandatory purple team exercise after an external test with limited to no vulnerabilities demonstrated will serve no value to the external testing team or the financial entity. We recommend that purple teaming is only required when a sufficient number of vulnerabilities are demonstrated in the red teaming exercise. This could be agreed by the TLPT authority with the financial entity enforced with outlining why a purple teaming exercise would not yield any benefit to the firm.

TIBER-EU's encouragement of purple team reflects the whole sector and does not relate to highly mature financial entities who already have sophisticated internal testing programs and we do not believe DORA's sets a sufficient mandate to enforce purple teaming across the financial sector. TIBER-EU's purple teaming guidance[1] states that, in order for purple teaming to be successful, there needs to be a clearly defined "scope, goals, objectives, timing and rules" and it is only appropriate in "certain circumstances." Mandating purple team exercises, without prior agreed objectives on the basis of the red team exercise, is unlikely to result in a useful outcome. We propose the following amendments:

[1] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_purple_best_practices.20220809~0b677a75c7.en.pdf

Recital 19: "… purple teaming. A purple team exercise can be waived by the TLPT authority if the control team determines that there is limited benefit to the financial entity if minimal vulnerabilities were found during the red team exercise."

Article 9(5) and 9(6): "… during the active red team testing phase. Where limited vulnerabilities have been identified and the control team, blue team and testers do not believe a purple team exercise would result in a benefit to the financial entity, the control team may contact the TLPT authority and waive the mandatory requirement to complete a purple team exercise."

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

Proportionality: The RTS includes the argument utilised by the ESAs for the identification of financial entities with proportionality applied. The rational provided states that the ESAs "give the competent authority the possibility to opt-in or opt-out financial entities based on specific features arising from the distinct nature of activities across different financial services sectors within the given criteria." While we understand the identification requirements, we note that the ESAs have not considered the operational structure of ICT systems for financial entities who operate across multiple Member States. In the majority of cases, mature financial institutions with multiple entities and branches will utilise the same ICT systems with central control and cybersecurity departments that administer their internal testing programs. A Member State TLPT authority could identify a financial institution based on a "specific feature" that would entail the exact same ICT systems and control procedures that have been tested by another TLPT authority. The argument used for the proportionality principle within the RTS does not relate to the operational practices of financial entities operating in the EU and **we recommend that consideration of the structure of the specific financial entity, alongside prior TLPT tests across other TLPT authorities, should be included within any identification.**

3. **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.**

Approach to identification: The ESAs approach to identification of financial entities uses the Level 1 text concerning the systemic characteristics of firms however we note that the consideration of firms based on "entities operating in core financial services subsectors" reflects the services that entities offer within Member States instead of the ICT systems that the TLPT will test. **There is a significant risk of material duplication in tests across TLPT authorities where the criteria for identifying a financial entity will choose to test the same ICT systems that the entity uses across all Member States.** We believe the identification of financial entities should focus on the ICT systems that the TLPT will test instead of using arbitrary criteria that do not relate to the TLPT. The RTS does note that "common ICT systems" will be considered in 2(2), however, we note that the financial entity is not able to participate in any consultation or challenge an identification on the basis of the TLPT relating to the common ICT system or having been previously tested. Financial entities are able to provide evidence that the ICT systems and control teams are common and that any proposed test could result in minimal benefit or information to the TLPT authority or financial entity. We recommend the following amendment:

Article 2(2): "… where these financial entities are established may, in consultation with the TLPT authority of the Member State where the parent undertaking of such group is established and the relevant financial entity, decide if the requirement…"

Common ICT systems and control teams: We note that the ESAs recognise that "common ICT systems" can be tested by TLPTs on multiple occasions and therefore mean a further TLPT will not be necessary. A further factor, alongside the same ICT systems, that the TLPT authority should take into account if they are considering a further TLPT is if the financial entity is using **common testing, control and cybersecurity teams to administer the TLPT**. A common ICT system alongside testing, control and cybersecurity teams further emphasises that a TLPT will result in the same outcomes with limited benefit to the TLPT authority or the financial entity. We recommend that this similarity is more accurately reflected in Article 2(2):

Article 2(2): … Where more than one financial entity belonging to the same group and using common ICT systems**, the same testing and cybersecurity teams to administer the test,** or the same ICT intra-group service provider meet the criteria set out in points (a) to (g) of paragraph 1, the TLPT authority(ies) of the Member State(s) where these financial entities are established may, in consultation with the TLPT authority of the Member State where the parent undertaking **or the most significant EU legal entity** of such group is established, **in consultation with the financial entity,** decide if the requirement to perform TLPT on an individual basis is relevant for these financial entities.

Article 12(3): For the purposes of conducting a joint TLPT in relation to more than one financial entity belonging to the same group and using common ICT systems**, the same testing and cybersecurity teams to administer the test,** or the same ICT intra-group service provider, the TLPT authorities of the financial entities performing such joint TLPT shall agree on which TLPT authority shall lead the TLPT.

4. **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.**

We believe the figure of EUR 120 billion of total value payment transactions may be too low and result in scoping in too many institutions. If the authorities choose to retain this figure, we recommend that the text be altered such that these criteria are not automatic causes for inclusion. Doing so would not limit the authorities' freedom to include financial entities in DORA testing, but would create greater flexibility for authorities to target only those firms they believe would benefit from such testing. We therefore recommend the following amendments to Article 2(1):

TLPT authorities shall **consider requiring** require all of the following financial entities to perform TLPT

From our experience, TLPTs can take significantly longer than the timelines envisaged in the RTS. This would be exacerbated if the inclusion of mandatory purple teaming is maintained. Further, in the event of significant findings, remediation of such technical issues could run beyond a year (noting that the financial entity is likely to implement compensating controls in the meantime). We therefore reiterate the importance of flexibility in

frequency of testing. At a maximum, the ambition should be to conduct a TLPT 3 years from the date of completion of the prior TLPT, not every 3 calendar years.

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

We wish to take the opportunity to reiterate the importance of a collaborative process between financial entities (FE) and TLPT authority for determining the selection of CIFs and supporting ICT systems which are to be included in the TLPT. DORA Art 26(2) makes clear that the FE shall determine which CIFs should be included in the TLPT and that this should be validated by the TLPT authority. However, Annex II 2(a) asks for information justifying why a CIF is not to be included in the TLPT. It therefore starts from the assumption that all CIFs should be included in the CIF. We do not believe this should be the approach as such an assumption could lead to overly broad testing scopes which would have a detrimental impact on the TLPT. Experience from past TLPTs suggests that a wide scope necessitates a more cursory test of the ICT systems that support the CIFs. For example, if a large number of CIFs are in scope, the TI provider will need to explore threats and available information for a much broader range of applications and businesses. To do so in the same period of time will necessarily mean the TI provider will not be able to go into the same level of detail that they would if the scope of the TLPT were a smaller number of CIFs. To achieve the objectives of a TLPT and meaningfully challenge an FE's defensive capabilities, depth is far more important than breadth of scope. We note that the scope of the TLPT is not currently covered by a Recital and recommend the following Recital be added to the text to clarify this point:

> [NEW] Recital 5(a): **The determination of the critical or important function or functions to be included in the TLPT is for the financial entity to make and to be approved by the TLPT authority. The scope specification document in Annex II requires the financial entity to provide a justification for its selection of critical or important function(s). As evidenced through the experience gathered in the TIBER-EU framework, setting an appropriate and limited scope for a TLPT is vital to ensuring adequate and safe testing. Therefore, financial entities and TLPT authorities should prioritise depth and rigor of testing over the inclusion of a large number of critical or important functions.**

Further, we believe the information required in Annex I and II may create confusion. In most cases, the FE will choose a small subset of CIFs for inclusion in the TLPT. Annex II 2(a) will therefore require a long list of explanations. In most cases, the reason for not including a CIF is likely to be repetitive (i.e. another CIF is preferred based on X reasons). Those reasons will likely relate to the CIF chosen, not the CIFs which are not chosen. We anticipate the FE needing to provide a repetitive list of explanations which will not be of value to the TLPT authority. We therefore suggest that Annex II 2(a) is deleted allowing the FE and TLPT authority to focus on the CIF(s) that have been selected for inclusion.

Further, Annex II does not currently account for previous testing which may be relevant in future TLPT. We therefore recommend a new 2(a) as follows:

> Annex II 2(a): **Where relevant, a list of critical or important function(s) previously included in the scope of a DORA TLPT**.

6. **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.**

Threat intelligence provider: The scoping guidance in the RTS does not provide clarity that the threat intelligence provider can also act as the tester for the TLPT. TIBER-EU does not mandate that the threat intelligence provider and the red team provider should be distinct, and we believe this should be further clarified within the RTS. TIBER-EU's procurement guidelines[2] provide significant detail regarding the interaction and collaboration required between both providers demonstrating the **significant gain in time and reduction in complexity** should they both be procured from the same provider. This has since become common practice within the financial sector. We propose the following amendment:

> Recital 14: … as a baseline for the national threat landscape. **The threat intelligence provider and tester may be procured from the same provider if the financial entity determines this is desirable, but must comply with all expectations laid out in this RTS and TIBER-EU procurement guidelines.**

7. **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.**

Alignment to TIBER EU procurement guidelines: As per the Level 1 DORA text, the financial sector supports the RTS' alignment to the TIBER-EU guidelines. The TIBER-EU guidelines for procurement, however, are prescriptive and DORA's mandating of TLPT across a wide range of financial sector participants would likely result in a **material stress being applied to the TLPT sector** and the number of experienced employees capable of meeting the procurement guidelines. In certain instances, the number of tests being administered across the EU may result in a financial entity not being able to procure in accordance with the criteria being mandated. In these circumstances, the safety of production systems must be paramount given the responsibility of administering the TLPT is held by the financial entity. **We recommend that the financial entity has the ability to delay a TLPT, in agreement with the TLPT authority, should the financial entity not be able to procure to a sufficient level of safety to perform the TLPT.** We propose the following amendment:

> Recital 9: … effective and most qualified professional services. **If the financial entity is unable to procure external providers who meet the requirements laid out in Article 5, the financial entity and the TLPT authority should consider a delay on the TLPT to allow further time for the procurement phase.**

8. **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.**

[2] https://www.ecb.europa.eu/pub/pdf/ecb.tiber_eu_services_procurement_guidelines.en.pdf

Response included in Question 7.

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

Red teaming timeline: The RTS requires the active red teaming test to be a minimum of 12 weeks. An arbitrary timeline for a test to take place does not reflect the variances in test times and the possible necessity of elongating a test unnecessarily. Testing, in addition, is secret and longer tests increase the difficulty to maintain this secrecy and therefore the benefit of the test itself. Any timeline should have flexibility to also be predicated on an outcomes-basis, and when both the entity and testing teams decide sufficient testing of ICT systems has taken place. A minimum timeline is arbitrary and we would welcome further flexibility within the RTS. We propose the following amendment:

> Article 8(5): "The duration of the active red teaming phase shall be proportionate to the scope and complexity of the financial entity and on the achievement of objectives in the red team test plan, and shall be based on a twelve week plan. The control team, the threat intelligence provider, the testers and the TLPT authority shall agree on the end of the active red team testing phase and if the red teaming phase should be reduced from twelve weeks subject to achieving the objectives stated in the red team test plan.

Critical systems: We note that paragraph 42 of the RTS references "critical systems". This is an undefined term and is not used within the DORA Level 1 text and may create confusion. Specifically, it is not clear whether the identification should cover which critical or important functions were covered, or which ICT systems supporting those functions. We recommend all terminology is consistent throughout the Level 1 text and the RTS as this can cause interpretation issues for in-scope financial entities.

TLPT approval: The RTS envisages a TLPT testing process that would place a significant level of responsibility on the TLPT authority to 'approve' or 'validate' various aspects of the TLPT for it to continue, and any changes, to the TLPT as it occurs. This will place significant burden on the TLPT authority, who could be administering multiple complex TLPTs at the same time, notwithstanding the potential additional complexity of the involvement of a third party provider or a pooled test. In total, during a test, the financial entity would be required to seek TLPT authority approval in ten circumstances (Article 6(1), 6(7), 6(9), Article 7(6), Article 8(3), 8(5), 8(6), 8(8), 8(9), Article 9(7)). **Without approval in quick succession, a TLPT will likely be stalled across multiple critical periods in a TLPT.** Noting the significant number of approvals already required by the TLPT authority, and that such approvals during the testing phases has often resulted in delays to the test, we therefore recommend that the TLPT authority should be informed, but not required to approve, any leg-up adaptions or additions. Instead, the conditions under which such changes are made should be part of the test plan to be approved by the TLPT authority. We therefore recommend the following amendments to leg up and detection-based approvals required by the authority.

Art 8(8): The control team shall timely provide leg-ups designed on the basis of the red team test plan. Leg-ups may be added or adapted upon approval by the control team **according to the conditions laid out in the red team test plan** ~~and the TLPT authority~~.

Art 8(9): In case of detection of the testing activities by any staff member of the financial entity or of its ICT third-party service providers, where relevant, the control team, ~~in consultation with the testers and~~ without prejudice to paragraph 10, shall **take** ~~propose and submit~~ measures **according to the conditions laid out in the red team test plan** allowing to continue the TLPT ~~to the TLPT authority for validation~~ while ensuring its secrecy.

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

DORA's requirement for pooled testing lacks sufficient detail and faces significant practical challenges for firms, regulators and third party providers. The majority of the issues listed below hold true in both a pooled and a TLPT involving a single FE and a third-party provider (TPP). Overall, we recommend that pooled or tests that involve an FE and TPP are not considered until TIBER-EU publishes guidance on those forms of test. We wish to note that other jurisdictions 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. 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 accountable for tests under the TLPT RTS, we do not believe the RTS provides sufficient certainty to allow entities to comply with a TLPT which included a TPP in its scope.

Preparation Phase

TPPs supporting CIFs: TLPTs are predicated on targeting "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 third-party providers who "support" CIFs, without any materiality threshold. Financial entities use a significant array of third-party providers to support CIFs. This could result in an 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.

Contractual challenges: In addition, financial entities utilise TPPs that vary in size, complexity and the services they offer. While the discussion has focused on cloud service providers (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 these contractual rights 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 noting that the scenario and specifics of the TLPT will not have been determined in prior negotiations nor specified within a contract. Any red team plan that includes scenarios with a third-party provider would require separate contractual negotiations (including NDAs) and planning between the financial entity and the third party provider. 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 Art. 6(9). In such a case, the FE would then need to renegotiate and amend legal terms with the TPP to achieve the changes. It would also need to discuss changes with the testers and TI providers which could impact on the contract between the FE and those providers. Should either the providers or the TPP object, the FE will be required to seek changes to the position of 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 significant uncertainties about how liability and risk management should operate in practice. For example, the FE's control team will not be able to conduct the risk assessment required in RTS Art. 5 or to manage the risks. If a control team is formed between all participants, it becomes unclear where responsibility ultimately lies for any impacts resulting from the test. This uncertainty is likely to serve as a significant barrier to contractual agreements between the FE and various other parties, whether TPPs or other FEs.

Choice of TI providers and testers: The preparation phase requires financial entities 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 wish to exercise veto rights.

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.

<u>Testing Phase</u>

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 of the terms of the test or considerably delay progression of the TLPT.

Control team: There is significant uncertainty 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, Non-Disclosure Agreements (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.

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.

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

Policy for the management of internal testers: The Consultation Paper in 52(a) notes that the financial entity will have to "define a policy for the management of internal testers in TLPTs." we would welcome clarification that this only relates to DORA TLPTs and not the group-wide internal policy for the financial entity's red team. Internal teams undertake other testing activities outside of the remit of DORA and those activities should not be included within a defined policy. We recommend the following amendment:

> Article 11(1): **For the purposes of this Regulation,** Financial entities shall establish all of the following arrangements for the use of internal testers **when conducting a TLPT in accordance with Regulation (EU) 2022/2554**."

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

Cooperation between TLPT authorities: The RTS does not include information concerning the scope of a TLPT should it entail multiple TLPT authorities. An expanding scope, due to multiple TLPT authority perspectives, would serve to elongate any TLPT and increase the complexity of a test. There should be greater clarification

that any expansion in authorities being involved in a test does not result in a material change to any scope or duplication of efforts. The financial entity, in addition, should still be allowed to respond to any scope to ensure the test remains rational to their operations across Member States. All financial entities in-scope of DORA TLPT have centralised security teams who operate across all Member States, alongside utilising the same ICT systems and controls. Adding applications on the basis of their use within Member States would not result in idiosyncratic responses per application and will only result in increasing complexity and difficulty in administering a test. We recommend the following amendment:

> Article 12(1): "(c) consult the financial entity concerning whether other TLPT authorities could be opted-in or if their operations in other Member States constitute common ICT systems, internal teams and or the same ICT intra-group service provider. The financial entity should provide evidence where cooperation could be appropriate to the TLPT authority."

Mutual recognition: The financial sector supports the proposed RTS's mutual recognition of TLPTs across Member States. Nonetheless, Article 12(5) only appears to support mutual recognition on the basis of "critical or important functions… internal testers… and if the TLPT was performed as a pooled test." All three criteria are not the only criteria to be considered for recognition and do not emphasise the most important factor for recognition – whether the TLPT tested the common ICT systems that the financial entity utilises between the two Member States. We propose that 12(5) should be amended to reflect this importance. In addition, we do not believe that report referred to in Article 26(6) and reflected in Annex VII 'Details of the test summary report of the TLPT' provide sufficient information for a mutual recognition determination to be adequately considered. We propose that the summary report includes a distinct mutual recognition amendment whereby a financial entity can provide further detail as to whether common ICT systems were tested that are equally utilised by the financial entity in other Member States.

> Article 12(5): "…functions, the use of common ICT systems and relevant internal teams, whether internal…"
>
> Annex VII Details of the test summary report of the TLPT: "(p) relevant information pertaining to the mutual recognition of this test across other Member States that the financial entity operates."

Mutual recognition within DORA does not reference recognition of other authorities outside of the EU. The EU via TIBER-EU has been engaging with other authorities on a cross-jurisdictional basis, as demonstrated by the G7 Fundamental Elements on TLPT and CBEST occurring alongside the ECB in 2021. We encourage any means to push for greater alignment across jurisdictions.

13. 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.

Threat intelligence report: Statements concerning the threat intelligence report within the RTS seem to suggest that there is more substantive information included within reports than is commonly the case. Recital 16, for instance, allocates specific time for testers to understand the threat intelligence report. These reports

are more generic and will not require allocated time for testers to understand the information provided. We would suggest that the time requirement is removed to allow the TLPT to be undertaken at a quicker pace.