DORA - Draft RTS (Second Batch)

Draft Regulatory Technical Standards specifying elements related to threat led penetration tests

March 2024

Executive Summary

AFME welcomes the opportunity to respond to the Draft Regulatory Technical Standards (RTS) specifying elements related to threat led penetration tests. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors, and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

Our response to this consultation is from the perspective of our bank members, focusing on those issues which are most relevant to wholesale capital markets. We are responding to each of the specific questions set out in the consultation paper, but wanted to raise the following overarching points:

1. **TLPT should be a learning exercise for tested entities, rather than a tick box regulatory exercise. This is best ensured by allowing firms a degree of flexibility in how to conduct the testing, for instance with respect to the use of purple teaming or internal testers.**

TLPT has been developed as an advanced and challenging form of testing, which helps to proactively identify potential weaknesses within a firm's risk management framework. Such vulnerabilities should be viewed as learning opportunities rather than for purposes of supervisory enforcement. This will ensure that the exercises are embraced by industry in the most open and challenging way. The increasing levels of prescriptive direction from authorities will inevitably result in a change of mindset, and lead to firms becoming more defensive and herding around certain specificities. One key example is the mandating of purple teaming, which should be at the discretion of a financial entity to enable them to respond to unanticipated eventualities, for example the exercise being detected as a test. Similarly, and regretfully, there is the restriction on significant credit institutions from being permitted to use internal testers. By failing to ensure that such in-house expertise is fully leveraged, TLPT is framed as an enforcement tool, rather than learning exercise. This should be revisited at the earliest opportunity.

2. **The expansion of TLPT across multiple parties, for example through pooled testing, is causing significant concern and should not be implemented without further guidance.**

The inclusion of third-party providers or potentially multiple financial entities (FEs) within one "pooled" exercise is a substantive expansion of TPLT scope and ambitions. While we welcome the concept of pooled testing in theory, such exercises will come with a range of new risks and legal complexities, identified further in our responses to the consultation questions below. We stress that such an expansion should be accompanied by additional guidance, addressing the coordination between entities, ownership, contractual restrictions, and subsequent combined remediation, to be developed in collaboration with industry. Again, there is a risk that such exercises significantly lose value if all involved parties are having to restrict engagement and openness, for fear of breaching contractual or commercial

restrictions over data confidentiality. The industry firmly believes that as currently articulated it would be highly unlikely that a pooled or third-party provider TLPT could be concluded successfully or within the timelines of the DORA regime.

Please see below our responses to questions 1 – 13. We remain available to discuss further any points raised.

Consultation Questions

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

- No objections. The alignment with the TIBER framework is supported in principle.

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

- AFME strongly supports the principle of proportionality. We are however concerned that the draft RTS does not apply this principle sufficiently rigorously. In particular the decision not to permit internal testers by globally significant credit institutions would fail to leverage the level of expertise which has been carefully developed in recent years within these firms. In the field of cyber risk such expertise is limited and hard-sought. Where a firm has internal resources in this area they should not be overlooked, especially where there are possible concerns on the availability of external testers. Another example would be the rigid application of timeframes, especially on red team testing, which go beyond the TIBER expectations and fail to provide discretion for the financial entity to react to unforeseen events or delays.

- Further, we note that the exclusion of only microenterprises creates the possibility of a very large number of financial entities being required to complete TLPT under DORA. While we support the criteria for inclusion given in Article 26(8) of DORA, we are concerned that the inclusion of a large number of firms would challenge the proposed frequency. We note paragraph 11 of the consultation paper, which signals that TLPT authorities will have flexibility in setting the frequency of these exercises. We support this flexibility and caution against the rigid enforcement of a 3-year rotation. We further suggest that NCAs retain the ability to reduce the number of firms in scope beyond what is given in paragraph 27. In particular, as discussed below in questions 3 and 12, opting out branches of larger financial entities in favour of a focus on the most significant EU entity of the group is seen as a practical way to reduce the number of firms in scope while achieving the same risk assurance. This approach would make the frequency proposed in the Level 1 text more achievable.

- Additionally, AFME proposes amending Article 2(3)(b)(h) to refer to the *complexity* of firms' ICT security detection and mitigation measures, rather than the maturity, to avoid creating a disincentive for firms to develop their approaches. We also recommend provisions within the tiered approach to encourage less mature entities to improve their digital operational resilience.

Question 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.**

- As AFME represents wholesale capital markets, the bulk of our members are within scope of TLPT. That said, we believe it is important for TLPT authorities to retain maximum flexibility regarding the number of FEs included in testing in order to not breach their intended frequency. To achieve this, the two-layered approach is appropriate. However, we believe that the exclusion of branches belonging to a wider group should be given greater weighting.

- Our members are concerned that the approach to identifying financial entities may in particular not fully take account of the group structure of globally significant credit institutions. Most of these FEs will have within their structures both regional branches and other types of legal entities operating within the EU. In the majority of cases, mature financial institutions with multiple entities and branches will utilise common underlying technology infrastructure with central control and cybersecurity departments that administer their internal testing programs. Financial entities should be able to flag to authorities where such underlying linkages exist for the purpose of avoiding overlapping exercises. As currently proposed, a TLPT authority could identify an FE for inclusion based on a "specific feature" with the result that the exact same ICT infrastructure and control procedures that have already been tested by another TLPT authority are subject to an additional TLPT. This will add no value for the FE and largely be a duplication for the TLPT authority, wasting limited resources, and replicating the risks of TLPT for no benefit. We would encourage permitting as much as possible TLPT on a joint inter-legal entity basis, so capturing both local and group scenarios. In this way resources can be optimised while satisfying TLPT requirements (see Q12).

- A further factor, alongside the common underlying technology infrastructure, that the TLPT authority should take into account is whether the financial entity is using common testing, control and cybersecurity teams (defensive capabilities) to administer the TLPT. Testing the defensive capabilities, not only the technical controls of individual ICT systems is a core objective of TLPT testing and therefore duplication of defensive capabilities is a relevant consideration as it increases the chance that the TLPT yields no unique results and will therefore be of limited value to the FE or the TLPT authority.

- We recognise that Article 2(2) acknowledges common ICT systems. Yet we believe the risk of duplication, and the negative resourcing consequences that could have for both FEs and TLPT authorities, warrants a more collaborative approach between TLPT authorities and FEs. In particular, it is essential that the FE is able to provide TLPT authorities with information regarding the potential overlap of ICT systems and controls in scope of any proposed exercise. We recommend the following amendment to Article 2(2) and corresponding amendment to Article 12(3):

    - Article 2(2): … Where more than one financial entity belonging to the same group and using common ~~ICT systems~~ **underlying technology infrastructure, the same testing and cybersecurity teams to administer the test,** or the same ICT intragroup 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~~ **underlying technology infrastructure, the same testing and cybersecurity teams to administer the test,** or the same ICT intragroup service provider, the TLPT authorities of the financial entities performing such joint TLPT shall agree on which TLPT authority shall lead the TLPT.

- Additionally, Article 2(2) assumes that the parent undertaking of a group of financial entities is based within the EU. This fails to accommodate those entities where the parent undertaking is outside the EU, or a multi-IPU structure is leveraged. Recognition of these structures would allow for more efficient and effective testing of common underlying technology infrastructure, with reduced risk to the organisations in question. This would, however, require an alternative approach to identification of the lead TLPT authority, such as designating the TLPT authority of the largest entity by balance sheet size within the broader group. Our amendment attempts to account for this through inclusion of a clause referring to the most significant EU legal entity of the financial group.

Question 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**.

- From our experience, TLPT exercises 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 FE 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. There should also be a guarantee to avoid the execution of TLPT exercises across a group's legal entities all in a single year, so providing benefits in terms of resource optimisation and ensuring project oversight capability.

- Allowing greater flexibility in the choice of FEs to undergo testing may be mutually useful to the authorities in managing potential resourcing strains. We therefore suggest an amendment to Article 2(1) which would not limit TLPT authorities' freedom to include FEs in DORA TLPTs, but would create greater flexibility to target only those firms they believe would most benefit from such testing:

  - Article 2(1): TLPT authorities shall **consider requiring** ~~require all of~~ the following financial entities to perform TLPT:

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

- AFME strongly welcomes the decision to incorporate the use of internal testers within TLPT exercises. This has long been an ask of our members, given the level of resourcing required to

perform these exercises and the pools of expertise within globally significant credit institutions. It is therefore highly regrettable that the proposal has not been extended to these entities and we would urge the ESAs to reconsider at the earliest opportunity.

- We are otherwise in favour of close alignment with the existing TIBER process, given the level of familiarity which has been built up regarding that framework. We would strongly urge the ESAs that where they have decided to go beyond the existing practice, and include additional aspects, for example on pooled testing, this is accompanied with a set of guidelines on how firms should apply these new requirements. There is a lot of uncertainty on how these extensions would work in practice which is not addressed within the draft RTS. Please see Q10 for our specific concerns on pooled testing.

- We also flag that there is similar concern over the broader proposal to include third party providers within TLPT testing, in addition to pooled testing. There is a high degree of scepticism at the value of including third party infrastructure within testing by the FE, as it will only lead to a less open and transparent environment due to the inevitable need for additional safeguards around access to systems and databases. Financial entities have also developed other means by which to identify and address potential vulnerabilities within third party providers, for example information security due diligence questionnaires. These are more appropriate vehicles of risk management, than combined participation in TLPT. Including third parties in a TLPT exercise will additionally present a significant challenge on coordination, potentially across hundreds of entities if the exercise has not been carefully targeted in scope. To ensure such testing is feasible, and focused on those material third parties who have the necessary resourcing capabilities, we call for operational guidance to be developed ahead of any exercises with providers being rolled out across industry.

- We do though welcome the proposal for any additional requirements to be carried back across in due course to the TIBER framework, so that in future the two frameworks are aligned and consistent.

- We wish to take this space to reiterate the importance of a collaborative process between the FE and TLPT authority for determining the selection of CIFs (Critical and Important Functions) and supporting ICT systems which are to be included in the TLPT. DORA Article 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 TLPT. 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 exercises 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 threat intelligence (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 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 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 Annexes 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.

Question 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**.

- AFME members are familiar with TLPT exercises and the related risk management requirements associated with performing these exercises, both in advance and during the exercise. There remains a number of sensitive areas which continue to demand extra attention, especially around production data disclosures. The key point we stress though is that such experience has identified occasions where the risk from continuing with a TLPT exercise would outweigh the potential benefits from any lessons learnt. Such experience is best leveraged from providing financial entities flexibility in how they implement the risk management requirements, using a risk-based approach. Please see Q7 for our thoughts on the new elements being proposed. We propose that the risk analysis findings should be clearly documented in a commitment letter to serve as an agreement that outlines the scope of the tests, the roles and responsibilities of the red team, the relevant authorities, and any third-party providers involved. Such an approach ensures that all parties have a mutual understanding of the testing parameters and the associated risks.

- One issue where further clarity is though sought, is how the requirement on indemnity insurances applies to a pooled exercise with multiple entities.

- We also flag that the scoping guidance in the RTS consultation does not provide clarity that the TI 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[1] provide significant detail regarding the interaction and collaboration required between both providers

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

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 an amendment to Recital 14 to ensure clarity on this point:

- 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.**

Question 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**.

- It is currently proposed under Article 5(2)(h) that external testers would be involved in *restoration procedures*. We would suggest this term is replaced with the term *clean-up procedures*, limited to the exercise itself, as a firm's full restoration of any impacted systems would be out-of-scope for external individuals.

- We also recommend amending the prohibition under Article 5(2)(i)(iii), to stress that there should be no intentional compromise of any function, not just critical and important ones:

  - Article 5(2)(i)(iii): intentionally compromising ~~the continuity of critical or important functions of the financial entity;~~ **the service availability or continuity of any function of the financial entity with no authorisation**.

- More generally, we caution that DORA's mandating of TLPT across a wide range of financial sector participants will likely result in a material stress being applied to the TLPT sector and the number of experienced employees capable of meeting the procurement guidelines. We anticipate a significant rise in the cost associated with procuring such services which may adversely impact smaller financial entities. We also anticipate that there will be an increased demand for such skills by financial entities which will likely choose to source from the threat intelligence or testing providers leading to a resource challenge for those providers. 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 to 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 testers 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.**

Question 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.

- While noting the alignment with TIBER's Services Procurement Guidelines, the proposal for the staff of both threat intelligence providers and external testers to have at least 5 years' experience feels an overly arbitrary metric, which may impact on the availability of testers, especially in a market with fiercely sought-after expertise. Given the expansion in scope of tested entities, it is also very possible that requirements which were not previously an issue could become one in future under DORA. We would therefore ask for greater flexibility in procuring such testers, including the ability to delay TLPT exercises if suitable personnel cannot be reasonably identified or in the event that a concentration risk is arising. Similarly, the requirement for threat intelligence staff and testers to have participated in a specific number of assignments is somewhat arbitrary and could likewise be replaced with the requirement for firms to assess the suitability of their staff prior to testing. As a minimum, it would be helpful for the ESAs to clarify that the requirements around participation in prior assignments is not limited to DORA specific assignments, as such a limitation would effectively prevent firms from conducting testing from the outset.

- Alternatively, and potentially even in addition, there is considerable interest in the idea of accreditation for testers, especially given the information and data which these individuals will inevitably have access to, including potentially high levels of sensitivity. The accreditation could take the form of a Code of Conduct or Ethics for such personnel, or alternatively assess the maturity of the company and their screening of staff. Such an accreditation would prove a more meaningful benchmark of quality assurance than a set number of years' experience and could be centrally maintained along with a list of accredited testers. This will improve the level of trust and it is worth noting this approach is already in practice in the UK, where the Bank of England (BoE) has worked with CREST on developing accreditation standards for those involved in CBEST[2]. Aligning with these accreditation schemes, rather than requiring individuals to have a specified length of experience, is also more innovation friendly, foreseeing the possible future introduction of AI or other forms of new technologies in this space. Given the tight timeframes for DORA, and the time it would take to adopt such accreditation standards, it is proposed at this stage the RTS simply takes account of their possible existence in future, as a suitable alternative to the outlined metrics.

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

- While AFME members are comfortable with the proposed timeframes, as default standards, there is concern over the level of flexibility in the event of unforeseen circumstances, for example the lack of availability of external testers. The ability to deviate from these timeframes may be necessary to ensure that the exercise can proceed with all quality assurances fully leveraged. A number of AFME's members flagged that past experiences have shown missed opportunities for greater learning and evolving by their strict adherence to specified timeframes, which left the authorities unable to fully engage to the depth which would have been welcomed. For international firms in particular, there is a risk that TLPT exercises on common underlying technology infrastructure could be driven out of other jurisdictional requirements, which could overlap with proposed TLPT exercises in Europe.

[2] https://www.crest-approved.org/membership/cbest/

Running overlapping TLPT could generate substantial additional risks and could jeopardise the integrity of the testing. Including a provision allowing for a deferral by a specific time period (e.g. 6 months) in extenuating circumstances to account for such circumstances would allow firms to manage these risks and avoid conflicts between testing regimes.

- It may also be to the benefit of authorities, who should likewise be subject to default timeframes in terms of scope approvals, in that added flexibility or discretion would provide more opportunity for their involvement across the process. 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 progress, as well as 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. The complexity of managing this would increase significantly in a pooled test scenario owing to the need for coordination between the multiple FEs involved. To address this risk, TLPT authorities should consider firstly allowing the control team to have a greater independence of decision making and secondly holding further pre-emptive discussions with the FE on the conditions for such decision-making including example scenarios.

- Flexibility should likewise be adopted with regards to purple teaming, which can be an important means by which financial entities can extract value from a test where the secrecy has been compromised, but where nevertheless failing to obtain lessons from the level of resourcing at stake would be incredibly wasteful. Rather than mandating purple teaming, we recommend flexibility as to how this valuable tool is deployed, with firms best placed to gauge, taking account of their varied operating models. The timeline for purple teaming should also appreciate the need for pauses in activity, for example if testers are detected or if support is needed from the firm to provide the testers with a foothold in the environment.

- Further to this point on how the authorities will be engaged, as part of the proposed testing methodology, we would seek clarification on how the remediation plans will be monitored and pursued by authorities in the follow-up to any TLPT exercise. There is no specification regarding the remediations oversight from the authorities. This should be better specified. As mentioned throughout, AFME members are keen to see these exercises fully maximised as a learning opportunity, with all stakeholders drawing out actionable conclusions which can be fully embedded in operations going forward. To this end, there must be time for financial entities to implement such actions, potentially with assistance/assurances from authorities. If the attention were to immediately switch to the next TLPT exercise, it would not only impede such implementation but signify that TLPT had become a tick-box mentality. We also propose the test summary report be shared together with the remediation plan, and not in advance as proposed in Article 9(7).

- Additionally, we flag the proposed timeframes appear to be uniformly applied to all forms of TLPT, for example also to testing with third party providers and pooled testing, despite the additional challenges from a resourcing and coordination perspective. Given the added considerations, such exercises require an adjusted approach, and we call for the ESAs to develop specific guidelines to this effect. Please see Q10.

- Specifically on red teaming, we recommend the following:

i. The industry believes that greater flexibility should be built into the 12-week timeframe provided in the RTS to ensure the testing duration can be adapted to reflect the level of complexity of the exercise itself. In particular, we believe that a focus on outcomes and objectives should be primary when considering when to end a red team test. The specification of time duration of activity is also not sufficient in that in fails to capture for example that some scenarios can run in parallel, thus reducing the needed testing time. It is indeed entirely feasible that red team testing could be completed in less than 12 weeks, especially depending on the number of individuals allocated to the exercise. In such an instance there should be flexibility to conclude this phase early – the ad-hoc creation of new tests could generate additional risks for firms and could compromise the integrity of the testing process. This flexibility in testing duration would also better recognise the differing levels of resource across firms of different sizes and maturities. One additional proposal has been to specify that the 12-week duration is on the basis of X number of FTEs (Full Time Employees), and that financial entities can reduce the duration by increasing the number of FTEs. Such flexibility would take into consideration the size of the organisation's selected targets and a realistic attack path. This would allow in-scope organisations to scale up or down on the various stages of the test as appropriate. 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,** ~~in any case shall at least be~~ **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**.

ii. Past experience has shown that leg-ups will be required by testers to make progress toward the objectives of the test. We welcome the acknowledgment in Article 8(2) that the red team test plan should include consideration of when leg ups are to be provided. However, experience has shown that addition or adaption of such plans is frequently necessary as it is difficult to anticipate the exact circumstances that the red team test will lead to. 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 amendment:

   - Article 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~~.

iii. We believe that detection of testing activities will become increasingly frequent as FEs become more sophisticated in their defensive capabilities. Already, multiple FEs

report that maintaining the confidentiality of the test is technically challenging for an FE due to the difficulty providers have in creating the appearance of a true external adversary. Typical external testing methodologies involve the provider making use of a number of legitimate third-party services which only allow the provider to conduct testing activity on other firms with the proper documentation. Examples of testing activity that the third parties would require to be registered include sending phishing emails from a public cloud infrastructure or utilizing public cloud storage instances to capture and replay credentials. Testing providers have registered their business activity with these third parties to ensure they do not suffer operating impact due to abuse reports filed with the third parties by the firms undergoing testing. From the standpoint of the blue team, with no knowledge that the FE is undergoing a legitimate test, detection of the provider's testing activity conducted using such third-party services appears to be abuse of those services. In an FE with sophisticated defensive capabilities, the standard response would be to utilise the relationship with those third parties to seek to disrupt the perceived adversary activity at its source. For example, the blue team full mitigation of the testing activity observed could involve significant escalation within the third party to have them take action against the activity being observed on their platform. This is a proven approach which the blue team would expect the third party to action. However, as the testers activity is registered as "legitimate", the third parties are unlikely to actually take action against the activity reported. This inaction would be confusing to the blue team which would rightly conclude that the platforms would only allow legitimate activity to continue. Once this is established it makes it very challenging to maintain appearance of a real, targeted adversary. In these circumstances, in order to maintain confidentiality, it is necessary for the control team to make quick decisions in order to respond to blue team activities, for instance halting the normal contact to the third party cloud company in order to avoid discovery by the blue team that the threat actor is legitimate. The speed at which these decisions need to be taken to maintain confidentiality do not fit with a model where the FE is expected to clear decision making with the TLPT authority and wait for confirmation. We suggest the following amendment to allow the control team to take decisions unilaterally to preserve the confidentiality of the test:

- Article 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.

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

- The primary ask is that before any application of pooled testing, the ESAs or other competent authorities produce guidelines in addition to this RTS (akin to those produced for purple

teaming[3]) to clarify how these exercises would work in practice and how to tackle the additional risks associated with data and information flowing across multiple entities. In particular, we would ask for guidance covering the following:

- **Documentation & Contractual Challenges**: The wording of paragraph 11 of the draft RTS consultation refers to a "designated financial entity" being in charge of providing all necessary documentation and monitoring the test. This could be read to imply that an individual "designated financial entity" would bear responsibility towards the other financial entities in scope of the pooled testing for the provision of documentation and monitoring of the pooled tests. Where the FEs are not part of the same group this would put an undue liability on a single financial entity, and we would propose that the ESAs clarify that each financial entity in scope of the pooled testing is responsible for the provision of their documentation, and to conduct their own monitoring. 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 third-party provider. 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 Article 6(9). In such a case, the FE would then need to renegotiate and amend legal terms with the third-party provider to achieve the changes. It 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 third-party provider 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. Indeed, given that TLPT authority approvals are required throughout the testing phase and involve fundamental elements of the test, such as leg ups or actions to maintain confidentiality, it appears likely that delay is inevitable without a revised, streamlined approach. Finally, as discussed above, we seek clarification on how indemnity insurances would work in this pooled context.

- **Ownership**: It is not clear who is responsible for owning the exercise and assuming ultimate responsibility for the control team. We acknowledge the Level 1 text states the third-party provider will directly procure an external tester but are unclear whether this shifts the burden of responsibility completely onto the provider. Specifically, we flag:
  - **Accountability and risk assessment**: The financial entity in the RTS is responsible for all risk management of a TLPT and is required to conduct

[3] TIBER-EU, Purple Teaming Best Practices, July 2022, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_purple_best_practices.20220809~0b677a75c7.en.pdf

a full risk assessment. The inclusion of third-party providers in a TLPT, or a pooled test scenario, creates 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 Article 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 uncertainly is likely to serve as a significant barrier to contractual agreements between the FE and various other parties, whether third party providers 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 Article 5(2)(e)(ii) and 5(2)(f)(ii). Further, it is unclear how to proceed if the FE and the third-party provider have conflicting views regarding the suitability of the testers or TI providers. This would be compounded in the case that multiple third-party providers 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.

- **Joint decision-making:** Assuming the third-party provider will be responsible for identifying the financial entities to participate within such an exercise, it is not clear if the financial entities will have the right of veto if they have recently performed a TLPT exercise on the underlying systems. Further, how will all parties agree and sign-off the scenarios without creating a circular series of changes and approvals between FEs, testers and third-party providers. This raises the significant uncertainly about how a control team would manage a test in a pooled test or in a TLPT with multiple third-party providers 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 / remediation plans:** 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. There is even uncertainty whether the remediation plan would be developed collectively with one output

having input from all parties (a significant operational challenge) or whether a series of separate plans by each of the entities is anticipated. Subsequently, it is 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.

- AFME is also struggling to understand the purported rationale for pooled testing, specifically that it should only be expected if non-pooled testing would have an adverse impact on the confidentiality of the data related to such services. Clarification on whose data would be impacted, whether the financial entities or the third-party providers, is sought. And who would make this determination. We also flag that 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 a impractically large number of third party providers 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.

- Finally, we recommend that given the scale of resourcing at stake in such collective exercises, and the level of coordination required, such testing should be valid for a longer period than is the case with regards to non-pooled testing. We specifically recommend that testing results from pooled testing be valid for at least a 5-year period, and sit alongside other measures where possible, for example due diligence questionnaires and tabletop exercises.

Question 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.

- The decision to exempt significant credit institutions from using internal testers is a sorely missed opportunity. As stated above, it frames TLPT not as a learning exercise but an enforcement tool. We call on this restriction to be revisited at the earliest opportunity, especially in light of the proposal within this consultation, for the TLPT innovations under DORA to be carried across into the TIBER framework. Any concerns over internal testers can be mitigated, for example by requiring periodic use of external testers, as indeed is currently proposed with other types of financial entities. Future flexibility over internal testers could also alleviate any bottlenecks which arise with regards to the availability of external testers.

- We also note Article 11(1)(a)(ii) requires internal testers to have been employed for at least 2 years before any involvement in a TLPT exercise. This seems both arbitrary and highly restrictive. Financial entities need greater discretion in deploying internal resources, with various supervision/governance safeguards providing sufficient quality assurance. The requirements of Article 11(1)(a)(i) already require firms to assess the competence of their testers, which would cover any issues in relation to the familiarity of staff with a firm's systems and is a much more appropriate approach to ensuring the competence of testers.

- We would additionally welcome explicit confirmation the policy relates only to internal testers for the purposes of DORA TLPT's:

    - 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**."

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

- Despite being highly supportive of the ESA's intentions to bolster supervisory cooperation in this field, we are concerned with the current drafting on how a home TLPT authority should reach out and notify TLPT authorities in other member states of an upcoming exercise. We would urge clarification that observer authorities should not be seeking to revise the proposed exercise's remit or specifications to prevent last minute changes which could cause delay or confusion.

- Additionally, while the current wording allows for TLPT cooperation, it does not require it. It would be helpful for the ESAs to more firmly encourage cooperation, for instance requiring that TLPT which can be conducted on a group-wide basis, covering subsidiaries, under a single lead TLPT authority should be done wherever possible.

- We note the RTS currently requires the home TLPT authority to make the determination of which other TLPT authorities should be involved. This is to be done on the basis of the CIFs operated in other member states. There are several concerns with this approach:

    - Beyond the operation of a CIF in another member state, it is equally important to consider whether the FEs operations in the host jurisdiction rely on the same underlying ICT systems and cybersecurity defensive capabilities, in particular the blue team. Many FEs in-scope of DORA TLPT have centralised security teams that operate across all Member States, alongside utilising the common ICT systems and controls. Because of this, including additional CIFs in the scope of the test on the basis of their use within a host Member States would not necessarily result in idiosyncratic responses per CIF and will only result in increasing complexity and difficulty in managing the TLPT for the FE and TLPT authority. It is therefore important to consider the use of common ICT systems and defensive capabilities.

    - Even if the CIF operating in the host member state is not ultimately selected to be in scope of the TLPT, the test may nevertheless be highly relevant for the host member state in terms of the ICT systems and defensive teams tested. Successful completion of the test, even without a local CIF in scope, should therefore give the host TLPT authority significant reassurance regarding the cybersecurity of the financial entity thereby justifying mutual recognition.

    - Given that the information we describe in point 1 above will not be immediately apparent or obvious to the home or host TLPT authorities, the FE should be involved

in the determination of which other TLPT authorities should be invited to cooperate in the TLPT. The FE should make an initial recommendation to the home TLPT authority regarding which host TLPT authorities should be invited to participate or observe the TLPT. The home TLPT authority should validate this recommendation with reference to CIFs operating in other member states, and then initiate outreach to those host TLPT authorities.

We therefore suggest the following amendments:

- [NEW] Article 12(1.a): **Receive from the control team a recommendation for which TLPT authorities in host member states may be involved, taking into account the use of common ICT systems and defensive capabilities are operated in, or shared across, host member states.**
- Article 12(1)(a): determine which TLPT authorities in host member states may be involved, taking into account **the recommendation of the control team and** whether one or more critical or important functions are operated in, or shared across, host member states;
- Article 12(5): For the purposes of mutual recognition of a TLPT, the attestation referred to in Article 26(6) of Regulation (EU) 2022/2554 shall indicate the scope of the TLPT, including the reference to the critical or important functions in the scope of test, **the common ICT systems and relevant defensive capabilities that were part of the test**, whether internal testers were used, and if the TLPT was performed as a pooled test. Where relevant, the attestation shall include information on functions in the scope of the TLPT in relation to which the TLPT was not performed. Where relevant to facilitate the mutual recognition, TLPT authorities shall share relevant information relating to the TLPT carried out.

- In parallel, we thoroughly endorse the proposal to enable mutual recognition of testing results. It is very possible that for reasons such as resource availability, certain TLPT authorities may not be able to observe or participate in an exercise but may nevertheless wish to recognise the results in order to avoid conducting a duplicative TLPT. Alternatively, the TLPT authority may wish to exclude a financial entity where the use of common ICT systems and defensive capabilities between their home and host operations means that a TLPT in the host jurisdiction would be redundant or duplicative. Reviewing the summary report may provide this information for that host TLPT authority. This possibility is not adequately considered in Recital 5 where there is no reference to common defensive capabilities. We therefore suggest the following amendments:
  - Recital 5: Financial entities may be part of a financial group. Where such group includes other financial entities and uses common ICT systems **and defensive capabilities**, authorities responsible for TLPT matters should consider the group structure and systemic character at national or Union level in the assessment of whether a financial entity should be subject to TLPT. **TLPT authorities may also wish to exclude financial entities where other entities in their group have been subject to a TLPT and the host TLPT authority deems that test to be relevant based on information provided in the details of the test summary report of the TLPT in Annex VII.**

- Further, in order to ensure that all information necessary to make a determination of mutual recognition is included in the report summary, we recommend an amendment to Annex VII to include the additional information regarding the use of common defensive capabilities:

    - Annex VII Details of the test summary report of the TLPT: "(c) the validated scope, including the rationale behind the inclusion or exclusion of critical or important functions and identified ICT systems, processes and technologies supporting the critical or important functions covered by the TLPT, **and the defensive capabilities involved in the TLPT**;

- Additionally, to facilitate the information sharing required for mutual recognition, we propose developing a classified information exchange system. The system would provide an additional layer of security that is commensurate with the critical nature of the information being handled. This will enhance the trust and confidence of financial entities in the TLPT process while ensuring that the findings are relied upon as widely as possible.

- Finally, the draft RTS fails to make reference to the possibility of third country mutual recognition. Given the growing interest in TLPT across international bodies and authorities, we would strongly encourage a specific reference to the possibility of financial entities relying upon the attestations under Article 26(6) within third countries, especially given the potential for global organisations to rely on the same set of systems for services outside the EU. In parallel, EU authorities should explore entering into mutual recognition arrangements with third country authorities, and in the interim to take account of third country exercises when determining when and how financial entities must perform TLPT under DORA.

Question 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.**

- AFME also wishes to flag there has been uncertainty across industry relating to a number of the terminologies proposed in the consultation paper, specifically the definitions for *blue team* and *control team* which include the *staff of its third-party services providers*. The emerging understanding is that this refers to staff within a financial entity's intragroup providers where this is relevant, for example where the SOC (Security Operation Centre) function has been outsourced to an intragroup provider, and that it does not apply to other third-party service providers who are not part of the wider group. Clarification would be welcomed.

- There have additionally been calls for an onboarding period by authorities within the approach to enforcement, for example that FEs can rely on TLPT exercises conducted this year as valid until at least 2027.

Contacts

AFME	Stefano Mazzocchi	+32(0) 2883 5546	stefano.mazzocchi@afme.eu
AFME	Coen Ter Wal	+44(0)020 3828 2727	coen.terwal@afme.eu
AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/