Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA Batch 2 Policy Mandate

Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554 (JC 2023 67)

Date: 1 March 2024

EU Transparency register: 3505006282-58

Question 1:
Are articles 1 and 2 appropriate and sufficiently clear?

No

Proportionality: The RTS fails to apply an explicit proportionate and risk-based approach as the ESAs continue to broadly consider that: (i) all ICT services supporting critical or important functions carry the same level of risk (or importance) to an FE; and (ii) any subcontractor linked to an ICT service supporting, or supporting material parts of, a critical or important function as equal regardless of their role and potential impact to the delivery of services. The application of a materiality threshold in accordance with a proportionate and risk-based approach will ensure that FEs are able to identify and monitor the material risks along the subcontracting chain, and those subcontractors whose disruption or failure could lead to a material impact to service provision. This approach will also reflect the intention in the DORA legislative text for a proportionate approach to ICT third-party risk management.

This could be achieved by aligning the supply chain scope in this RTS with the final draft of the Implementing Technical Standards on the Register of Information ('Register ITS'). In the Register ITS, 'material subcontractors' is appropriately defined as "only those subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof…etc.". This application of materiality to the subcontractor population is important not only for the purposes of the register, but it also ties to risk management. We therefore strongly advocate for the supply chain scope of the Register ITS and Subcontracting RTS to be aligned and that the definition of 'material subcontractors' will be ported into the final draft of the Subcontracting RTS. This alignment would be essential for the consistent approach to and application of the Level 1 and Level 2 third-party risk management requirements. As such, all references to 'subcontractor' in the RTS should be understood to encompass subcontractors effectively underpinning ICT services supporting critical or important functions, or a material part thereof, i.e. 'material subcontractors'.

Article 1

Sections (f-h) of Article 1 seem redundant for the required risk assessment concerning material changes to subcontracting arrangements, as they specifically relate to the inherent risk rating and assessment of the financial entity's planned usage of the service provided by the third-party provider, not to the subcontracting aspect. It is suggested that the ESAs reassess and consider these subparagraphs for removal to appropriately streamline the requirements, noting that these are set out in Article 1 of the regulatory technical standard specifying the policy on ICT services supporting critical or important functions.

Article 2

Oversight on Group-Level Outsourced ICT Services: Entities that are part of larger groups, which outsource several ICT services to other group entities subject to DORA, require guidance on the extent to which they can rely on the oversight and due diligence performed by their parent or group entities on their own ICT services, as well as on those provided by subcontractors. It is crucial for the final RTS to clarify whether and how the oversight conducted by parent entities within the group, which are also under DORA's purview, can be deemed sufficient for the purposes of fulfilling the subcontracting entity's regulatory obligations under DORA.

Besides, FEs with subsidiaries outside of DORA's application perimeter (e.g. in a jurisdiction of the European Economic Area) face uncertainty regarding their obligations to perform oversight at the group level on ICT third-party providers (ICTTP) and subcontractors of these foreign subsidiaries, especially when these entities are not directly subject to DORA's regulations.

We recommend establishing provisions within the RTS that allow entities to leverage group-level oversight mechanisms to meet the standards and requirements set forth by DORA without necessitating redundant assessments, thus promoting efficiency while maintaining operational resilience.

Question 2:
Is article 3 appropriate and sufficiently clear?

No

The subcontractor risk assessment in Article 3 is not risk-based and includes a number of requirements that expand current regulatory expectations and industry best practices, without commensurate benefit to risk management. Without the explicit application of proportionality and materiality, the requirements in this RTS would apply to an unnecessarily broad scope of subcontractors. This situation risks undermining the effective and efficient management of risks that have the potential to materially impact the delivery of the contracted service, or that pose a threat to financial stability.

The expectation that FEs monitor and oversee subcontractors directly, including through intervention in third-party / subcontractor contracts, is not appropriate and should not be necessary given the FE's risk management framework which is underpinned by robust due diligence practices and supplier controls, contractual agreements and risk-informed oversight measures that are tailored to the level of risk and complexity of the third-party engagement.

Direct oversight of subcontractors can be resource-intensive, diverting attention and resources from strategic risk mitigation efforts of both financial entities and third-parties. A financial entity's third-party risk management program is the most effective way of ensuring risk management practices and

regulatory obligations cascade down the supply chain and that third-parties and their subcontractors are held to established standards, whilst the FE remains ultimately accountable for assessing the associated risks and compliance with its own regulatory obligations. These measures are upheld, and are enforceable, through the contractual framework between the financial entity and the third-party.

Specifically, we note that:

- **Article 3(c)**: This requirement is inherently problematic and risks overstepping established legal boundaries and principles that preserve confidentiality as between contracting parties. Such principles would typically limit a FE's ability to have sight of or access the contract between a third-party and its subcontractor. As such, this requirement is inherently problematic and puts at risk a FE's ability to comply with this clause. Any requirement seeking to achieve the appropriate contractual flow down of risk management obligations along the supply chain, should be focused on ensuring that the contractual framework between the FE and its third-party provides for the replication of certain clauses in downstream agreements. This would reach the same intended outcome, whilst remaining in line with accepted contractual legal principles.

Article 3(e): The expectation of ***direct*** oversight of subcontractors is not an appropriate or feasible regulatory measure. Direct monitoring and oversight of subcontractors can be resource-intensive and would divert risk-management resources away from targeting where the actual risk lies. An exhaustive risk management approach does not provide any meaningful benefit in terms of managing and mitigating supply chain risk. A financial entity's risk management program is the most effective way of ensuring risk management practices cascade down the supply chain through the third-party and that subcontractors are held to established standards, whilst the FE remains ultimately accountable for assessing the associated risks and compliance with its own regulatory obligations. This is because of the following measures:

- FEs implement comprehensive, risk-based due diligence processes and supplier controls that are upheld and are enforceable through the contractual framework between the FE and its third-party;

- Third-parties must seek approval or consent before engaging a 'material' subcontractor. This ensures a FE is able to identify, monitor and manage the risks associated with those suppliers which have the potential to impact the delivery of the service;

- Third-parties are required to due diligence their subcontractors and make the results of this due diligence available to the FE upon request. This is an important obligation for providing visibility into a FEs risk posture (as it feeds into the inherent risk assessment) and contractual flow down;

- the contract between FE and third-party can explicitly provide for the flow down of risk management and oversight obligations to the supply chain;

- FEs assess a third-parties' control environments initially at onboarding and periodically on an ongoing basis, at a frequency and rigor that is reflective of the inherent risk of the third-party engagement. Any deficiencies identified in the third-parties' oversight of its subcontractors are identified, and appropriate action is taken.

It is important to emphasise that the risk management framework, including through the direct relationship with the third-party, does not equate to the delegation of a FEs responsibility to manage subcontractor risk along the supply chain, but rather is critical to enabling strategic and effective risk mitigation practices. Third-parties are better positioned to manage and monitor their subcontractors

as they (i) have a direct contractual relationship through which they can enforce the cascading of risk management measures and (ii) have a clear understanding of their service, their control environments and how the use of subcontractors may impact the delivery of the service.

We would therefore strongly advocate for a balanced and outcomes-based approach that allows FEs to effectively manage supply chain risks, leverage robust contractual frameworks and third-party expertise, whilst remaining ultimately accountable for material risks and compliance with their own legislative and regulatory obligations.

Additionally, we inquire whether the requirements laid down in Article 3 (a), (b), (c), and (d) are cumulative and assessed in aggregation. It is suggested that the ESAs provide clarification on whether it is necessary to fulfil all requirements, including obtaining specific clauses, or if the Financial Entity can proceed with executing an agreement with the Provider despite not meeting certain conditions.

Question 3:

Is article 4 appropriate and sufficiently clear?

Yes

Article 4 highlights the need for the Financial Entity to explicitly outline in written contractual agreements with ICT TPSPs which critical ICT functions can be subcontracted and under what terms.

Question 4:
Is article 5 appropriate and sufficiently clear?

No

Article 5 requires that a financial entity must assess the entire ICT subcontracting chain and review the contractual arrangements between the third-party service provider (TPSP) and the subcontractor.

Article 5(1): As noted above, the RTS captures a very expansive supply chain scope by setting the requirements across the *entire* subcontracting chain, without the application of a materiality threshold. This would add significant complexity and burden to a FEs risk management practices, without commensurate benefit as it fails to target supply chain risks that have the potential to materially impact the delivery of the contracted service – and, in fact, would divert risk management resources away from focusing on where the real risk lies. There is no value in an exhaustive approach to monitoring and oversight of subcontractors and burdening FEs and third-parties with every decision related to subcontractor. FEs risk management frameworks are designed to ensure a comprehensive, risk-based approach to the management of supply chain risks.

Article 5(2): The expectation for the FE to monitor subcontracting chain through the review of contractual documentation between the third-party and its subcontractor is inappropriate, unnecessary and would introduce significant legal, commercial, and operational complexity.

Firstly, it puts at risk the core tenant of confidentiality as between contracting parties and could raise conflict of law considerations, such as antitrust concerns. It also raises the possibility of an impact to the core common law legal doctrine of contractual privity by giving an entity which is not a party to the contract between ICT service provider and its subcontractor visibility over and a say in contract formation.

Secondly, it should not be a necessary measure given the contractual framework between the FE and third-party which, as noted above, would provide for the cascading of regulatory and risk-management obligations along the supply chain in respect of material subcontractors. The regulatory focus should be on ensuring robust contractual frameworks focusing on outcomes-based measures that ensure effective risk-based oversight, whilst also allowing contracting parties the flexibility to negotiate and agree contractual terms.

Finally, this requirement would have a significant real-world impact, should thousands of financial services firms be required to intervene in contractual negotiations across the entire subcontracting chain. This would impose a huge administrative burden and potential industry-wide disruption.

Question 5:
Are articles 6 and 7 appropriate and sufficiently clear?

No

Article 6(1): The requirement to notify of material changes to subcontracting arrangements should be limited to material subcontractors (i.e. subcontracting requirements that could have a material impact on service provision or the TPs ability to meet its contractual obligations), reflecting a risk-based approach. Extending this requirement to all subcontractors would impose a substantial administrative burden without proportionate benefits to risk management.

Article 6(2): The requirement to provide risk assessment results to the third-party in respect of any notified material changes will create an administrative burden without proportionate benefits to risk management.

Articles 6(3) and (4): The requirement that financial entities have the right to approve or modify changes to subcontracting arrangements may be incompatible with the one-to-many nature of public cloud services and other technology providers, which service multiple financial entities from a single infrastructure. In service this model, the real-world impact of a service provider having to await and manage approval or non-objections from numerous financial entities would not only create a substantial administrative burden but could lead to the loss of access to key services, negatively impacting resilience and competitive capabilities. We therefore suggest this paragraph is removed and have proposed amendments to paragraph (4) which appropriately capture the notification process while reflecting the practical limitations of such models.

We therefore propose amendments as follows:

1) In case of any material changes to subcontracting arrangements, the financial entity shall ensure, through the ICT contractual arrangement with its ICT third-party service provider, that it is informed with a sufficient advance notice period to assess the impact on the risks it is or might be exposed to, in particular where such changes might affect the ability of the ICT third-party service

provider to meet its obligations under the contractual agreement, and with regard to changes considering the elements listed in Article 1.

2) The financial entity shall inform the ICT third-party service provider of **any objections to the proposed changes** (to delete: "~~its risk-assessment results"~~) as referred to in paragraph 1) by the end of the notice period.

(to delete: ~~"3) The financial entity shall require that the ICT third-party service provider implements the material changes only after the financial entity has either approved or not objected to the changes by the end of the notice period."~~)

4) The financial entity shall have a right to **either (a)** request modifications to the proposed subcontracting changes before their implementation **or (b) terminate the agreement** if the risk assessment referred to referred to in paragraph 1) concludes that the planned subcontracting or changes to subcontracting by the ICT third-party service provider exposes the financial entity to risks as specified in Article 3(1) that exceed its risk appetite.

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA Batch 2 Policy Mandate

Draft Regulatory Technical Standards: on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents

and

Draft Implementing Technical Standards: On the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat

Date: 1 March 2024
EU Transparency register: 3505006282-58

Question 1:
Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

No

We observe several challenges in the draft RTS:

- Ambiguity in Notification and Reporting Periods
- Operational Limitations on Timelines
- Weekend and Holiday Reporting Constraints
- Time zone Discrepancies
- Reporting Fields

Proposed Solutions to the Reporting Timeline Challenges:

Clarifying the Notification Window: We seek clarification on the allocation of time for notifying, classifying, and reporting incidents. The statement in the RTS is open to interpretation, leading us to inquire whether the 4-hour notification period should be included or excluded within the 24 hours after detection, for instance. In this regard, we propose removing the following phrase in Art. 6, p.1(a) make the statement clearer:

- the initial report shall be submitted as early as possible within 4 hours from the moment of classification of the incident as major, (to delete: "~~but no later than 24 hours from the time of detection of the incident~~").

We also seek clarification regarding the interpretation of the 24-hour timeframe after detection of the incident particularly during holidays or weekends, for instance.

Introducing Proportionality Based on Operational Sensitivity: We would welcome further proportionality on the timeline based (i) on the nature of the activities of the institution more or less time sensitive (e.g. a small size private bank does not have 24/7 capabilities for reacting to an ICT incident, a payment institution may require 24/7 capabilities to address online payments, while a custodian bank has only 10/5 capabilities due to "transaction processing cut-off hours"), (ii) dependencies on service provider/head office time zones and (iii) on the systemic impact. One possible option would be to allow "clock pausing" during out of office hours + weekend + bank holiday for neither 24/7 nor time-sensitive financial entities. The timelines, alongside the number of data fields, appear predicated on PSD2, which relates to payment-incidents only. Payment incidents correlate directly to immediate information, such as the number of transactions, clients affected and geographic location. This is not the case for other forms of financial services nor incidents that affect ICT systems or applications. ABBL encourages greater flexibility for financial entities in terms of both the timelines and the level of information required during the critical periods of incident response and recovery, notably the comprehensive number of data fields required within the 72 hours intermediate report.

Adjusting Requirements for Weekend and Holiday Reporting: We would like to reinforce the practicality aspect of timelines being working days vs. calendar days. Within calendar days the FE mays ensure better quality and timely allowing at the same for any follow-up questions and timely response to potential enquiries raised by ESA. Furthermore, the industry notes in 6(3) that the flexibility concerning the reporting of incidents in a weekend or bank holiday of the Member State of the reporting financial entity is not applied to significant credit institutions, where the incident affects another Member State or if the entity is systemic according to the competent authority by the national market. We believe further flexibility should be allowed for all financial institutions in relation to the submission of intermediate or final reports, especially if an incident happens in another Member State. Incidents can relate to ICT systems, or other Member State activities, that are not systemic in nature and do not reflect an essential service or commercial impact to clients and the operations of the financial entity. The ability to procure information during a weekend or bank holiday can reduce the level of information included within reporting and it does not relate to the ability of the financial entity to respond and manage an incident. We do not believe that the intermediate or final reports are required during a weekend or bank holiday.

Standardizing time zone References: Further clarification is required regarding the time zone that the financial entity should utilize for incident reporting. It is unclear if this should be based on the reporting financial entity, the Member State that is receiving the report or the location of the incident.

Streamlining Reporting Fields: Reporting clarification: We would welcome further clarification by ESAs concerning whether all fields should be reported in all reporting stages irrespective of whether the fields are relevant to the incident or if they are non-applicable. This informs how a reporting process and automation can occur and provides clarity for implementation purposes.

Recurring incidents: ABBL requests greater clarification from the ESAs concerning how financial entities should report recurring incidents. RTS text states that recurring incidents should be based on the root cause criteria listed within the incident template RTS, however, the high-level nature of root causes within 4.1 would result in a material overreporting of incidents. It is therefore highly likely that for any incident determined to be major there will be non-major incidents in the following six months

that have the same root cause. The RTS requirements for recurring incidents will therefore de-facto result in financial entities building a final report for most incidents, including those with only very minor effects, in order to aggregate impacts to determine if recurrence has resulted in a major incident. This creates significant additional work for incident management teams with no benefit to risk management. It is also likely to result in substantial overreporting of recurring incidents. It is unclear how recurring incidents should, in addition, be reported. Root cause is often determined at the resolution of an incident, which would therefore require a repeat of the same process.

We request that greater consistency between incident reporting classification criteria and the instructions or descriptions within data fields is maintained. The incident classification criteria for economic costs and losses clearly state that these "shall not include costs that are necessary to run the business as usual." This is additionally repeated withing the guidelines on aggregated costs and losses. We believe this should be further embedded within the costs and losses data fields (4.13-4.25) and, most notably, in relation to staff costs. The recitals could, in addition, confirm that all incident fields on costs and losses are in line with the proposed incident classification RTS Article 7 and Article 18(3) DORA.

Question 2:
Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Partially

From our perspective, we found that with regards to these data fields, some of them require a very broad and transversal collection of information within the entity, and we believe this might pose difficulty especially for smaller entities. Such entities may struggle to comply due to the diversified and detailed nature of the information required. For larger entities, obtaining this information could be an extensive project spanning across multiple departments.

We have concerns regarding the inclusivity of these requirements, as we would prefer to have the reporting framework tailored to accommodate the diverse needs of different entities, given their varying setups and business models. Therefore, we suggest considering a simpler format versus a more complex one, or perhaps a lighter, more diversified approach within this context.

2.6 Discovery of the incident: For the purpose of keeping the reporting template as simple as possible for any type of FE and needs, we would like to recommend the criteria to be align to the PSD2 "cause of incident" information allowing to provide information on externally or internally detected incident selection (process failure, system failure etc.). The criteria chosen by the ESAs concerning how the incident has been discovered are undefined and could be interchangeable. For instance, an 'IT Security' incident could relate to production management whereas 'Staff' could also relate to all criteria. We would welcome the reintroduction of PSD2 categories 'Detected Internal' and 'Detected External' to show how financial entities normally discover incidents in practice.

2.8, 2.9 and 2.10 Description of the incident: We recommend that data fields 2.8 – 2.10 are combined to one, single data field. Note that financial entities are likely unable to come to an accurate determination of the impact of incidents to other financial entities and third-party providers in all circumstances. Financial entities are highly unlikely to know the impact by the initial notification timelines and we recommend this requirement should be switched to 'Yes, if applicable' at this stage.

As incidents rarely affect other financial entities or third-party providers, we recommend that data field 2.8 is changed to 'Yes, if applicable' in all reporting stages.

2.11 Information whether the major incident has been recurring: It is unclear why 2.11 is mandatory for all report stages. We would like to recommend for the field 2.12. "Number of occurrences of the same incident" not to be mandatory but voluntary (as applicable). If a major incident is determined as major due to it recurring, then financial entities will report on that basis under 'Yes, if applicable'. We recommend the inclusion of this data field is switched to 'Yes, if applicable' across all reporting stages. Root cause is often determined at the resolution of an incident, and therefore likely within the final reporting stages of an incident. If the root cause is then determined to have recurred, per the RTS on incident classification, it is unclear if a financial entity must then repeat and aggregate the same incident it has reported on through the initial and intermediate reports. A financial entity will be unaware if an incident has a repeated root cause at the beginning of an incident and we recommend all references to recurring incidents are only included in the final report.

Question 3:
Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Partially

3.3 Date and time of occurrence of the incident: It is unclear how this data field relates to recurring incidents, and we welcome further clarification. As stated in the previous question, a financial entity would be unaware concerning the root cause repetition until the resolution of an incident. References to recurrence in the initial and intermediate data fields should be removed. We would like to consider renaming this field from "Date and time of occurrence of incident" to "Date and time of the beginning of the incident" as more practical for FE to report.

3.5 Date and time when services, activities and/or operations have been restored: We would like to suggest adding the following point to align to the requirement for intermediate report and suggest to amend field 3.5 to "Date and time when services, activities and/or operations have been restored or are expected to be restored" to allow for FE to notify if a status changed significantly or when other relevant status update is available, what does not mean that the incident might be fully restored/resolved at day 3.

3.6 Number of clients affected: Clients are not always affected by an incident and we recommend that this data field is switched from mandatory to 'yes, if applicable' in the intermediate and final reporting stage. We recognise that this field is mandatory within PSD2, however, PSD2 relates to payment transactions which have a logical attachment to clients being affected by incidents. DORA's incident reporting places in-scope a wider set of incidents, including internal system-based incidents, which do not always affect clients.

3.7 Percentage of clients affected: As per above, DORA applies to a wide range of incidents that do not always relate to clients. We believe all reporting stages should be 'yes, if applicable'.

3.15 – 3.16 Reputational impact: The criteria and contextual information included within the reputational reporting criteria are onerous and do not relate to the ability of the financial entity to respond to the incident. The information infers that the financial entity should be undertaking

significant research of local newspapers, blogs and social media platforms at all stages of responding to an incident, which would detract the financial entity from responding effectively to the incident at hand. We recommend that a determination for 'reputational impact' should be based on the national newspapers of the relevant Member State where the incident has taken place and/or financial news of note.

3.30 – 3.31 Affected infrastructure data fields: Financial entities are only fully aware of the impact and location of an internal ICT-system incident once the root cause of the incident has been reached. On that basis, we encourage that the data field is only mandatory in the final reporting stage as per the period when root cause is reported. If the financial entity is aware of the exact location of the infrastructure incident, then the financial entity is aware of the root cause of the incident. A financial entity would only be able to respond to 3.31 at the final stage of reporting.

3.35 Temporary actions/ measures taken: We recommend that the data field concerning temporary actions and the 3.37 field describing those actions should only be required in the final reporting stage. By the intermediate stage, the financial entity should be concentrating on responding to the incident and determining the most effective response. Actions will likely change materially through the reporting process and the intermediate stage will likely provide inaccurate information or out-of-date information. We recommend the reporting stage for intermediate is 'no' and the final reporting stage is 'yes, if applicable' reflecting instances whereby the incident did not require action on behalf of the financial entity (i.e. external events without an impact). In addition, the field choice of 'yes' in 3.36 does not relate effectively to the level of descriptions included within 3.38 (i.e. Disaster Recovery site activated). The descriptions in 3.38 infer a severe incident that is rare and we therefore suggest 3.37 should be a field for temporary actions taken in relation to a severe incident scenario.

3.38 – 3.39 Information on involvement of CSIRTs: It is unclear how the reporting authority will use the information in this data field. A financial entity is unlikely to itemize the actions of a CSIRT during an incident response and is unclear why a financial entity should be reporting on the behaviour of another Member State authority via an incident report. We suggest this data field is removed.

3.40 Indicators of compromise: A financial entity will be unaware of this information by the intermediate stage of reporting, and we suggest the data field is change to 'No'. The field should not be mandatory if 'cybersecurity' is chosen within 3.26 for the intermediate report as a financial entity will not have the level of information to report reliably, at this level of detail, at that reporting stage. The information requested is highly burdensome and will detract a financial entity from responding to the incident.

3.41 Vulnerabilities exploited: The reporting of specific vulnerabilities can include confidential information that represents a significant cybersecurity risk to financial institutions. Given the risk being placed on the financial entity, including examples of how to expose vulnerabilities within a financial entity, it is unlikely a financial entity will provide any sensitive information in the 3.41 data field. We recommend the field is removed or any information provided will likely be of limited use to the reporting authority.

Question 4:
Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Partially

As stated in the Executive Summary, AFME believes that the incident reporting regime for recurring incidents is highly burdensome for financial entities to implement. The incident classification RTS Article 15(1)(b) infers that the root causes in Data Field 4.1 will be used to determine if there has been a recurrence. The root causes listed, however, remain high-level and a small proportion of root causes, such as change management and software compatibility, will likely disproportionality trigger reporting on the basis of recurrence. An incident may have a change management root cause that is significantly different to another incident with differing incident management controls, processes or errors. As the stated purpose behind reporting recurring incidents is to indicate "significant deficiencies and weaknesses in the financial entity's incident and risk management procedures," we believe there should be greater recognition of the financial entity's ability to determine is a root cause has repeated. Recurring reporting, due to high-level root cause criteria, would result in material overreporting due to a concentration of incidents relating to specific causes and improper reporting due to a lack of direct link in incident management procedures between incidents. We therefore propose that a financial entity can determine when a root cause is recurring within the Data Field 4.3 and the Data Field 4.1 is maintained for normal incident reporting-only.

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

4.4 Information about inability to comply with legal requirements: A financial entity will not be comfortable hypothesising their potential legal exposure within regulatory reporting. There are material consequences to providing details regarding how a financial entity may have failed to comply with the law, especially if shared with their financial regulators and supervisors. Financial entities, when responding to ICT incidents, will focus on root cause identification, incident containment, remediation, and management of communications with and continuing to support our clients. An exercise of identifying all relevant regulations and their potential for non-compliance across all relevant Articles does not meaningfully contribute to common risk management practices or the resolution of the incident and the entity's services. We recommend that this data field is removed or it is unlikely financial entities will respond or will provide high-level comments only that will not provide the reporting authority with usable information.

4.5 Information about breach of contractual arrangements/ SLAs: It is unclear regarding how the information in the data field will be utilised by authorities and how the information correlates to the assessment of an incident and its impact. The content of contractual arrangements and SLAs do not relate to the materiality of an incident, the root cause or the entity's ability to respond to the incident. Contractual arrangements and SLAs are confidential and a financial entity would not provide details concerning confidential client information within regulatory reporting. As a financial entity will have to list client and financial counterparts within reports (3.6-3.10) and the costs of non-compliance (4.18), there is a risk that descriptions of contractual arrangements or SLAs could be linked to specific

clients of the financial entity. This could place legal risk on the financial entity if costs were able to be linked directly to a client. As the data field does not relate to the incident and could reflect confidential information, we recommend this data field is removed. In addition, it is worth mentioning that even at the final notification stage, in some cases, it would be hard for FE to make a direct connection between an incident and impact on SLA performance. Similarly, from the reporting timeline perspective, the impact on the performance might not yet be materialised/visible through the monitoring.

4.8 Date and time when the incident was resolved and root cause addressed: The date and time when the incident was resolved is distinct from the date and time when the root cause is addressed. It is not clear why these two distinct time points are allocated to the same data field. We recommend this data field is split into two data fields.

4.10 Information relevant for resolution authorities: The criteria included that would require the financial entity to contact the resolution authority are extreme incident scenarios which would likely results in a material interaction of supranational and national supervision teams engaging directly with the financial entity through the incident. It is highly unlikely for this extreme scenario to occur (i.e. one that impacts an entity's capital stack) and we recommend the field is removed or changed to 'yes, if applicable' in the final reporting stage.

4.14 – 4.23 Amount of costs: The level of information required for all data fields is highly onerous and would place a significant reporting burden on financial institutions to analyse incidents that could be vary significantly in scale. It is unclear concerning how this information would be used and why certain specific costs needs to be collected by authorities. The procurement of legal counselling, for instance, has limited relevance to incident response management and it is difficult to foresee how this information would be utilised by authorities. We recommend the cost analysis requirement are reduced significantly or changed to one data field-only. All examples in 4.23 are highly specific and do not appear to relate to incident management.

The classification criterion for Economic impact of an incident is not practical and adding complexity. Accounting and financial systems are not set-up the way to easily allocate the staff cost, communication cost and replacement costs directly to a single or aggregated incidents of similar nature. Hence, finding links to direct or indirect costs determination is problematic adding potential costs for enabling such tracking (if possible). In addition, the materialisation of some costs and timeframes obligations are not aligned e.g., fees, legal counselling or advisory costs associated with the incident. Such procedures are usually taking more time making it hard to be part of the classification and to be included in the annual aggregate cost and loss report.

Therefore, we propose a more simplified criteria approach as an alternative solution:

Having economic impact criterion at high-level and giving flexibility to the institutions which costs and losses are relevant for an ITC-related incident. We suggest removing direct and indirect parts and reword as suggested below:

- the economic impact, any relevant costs and losses incurred as a company consequence of the ICT-related incident.

4.18 Amount of fees due to non-compliance with contractual obligations: As mentioned within responses to 4.5, contractual obligations constitute confidential information and there is a risk that costs could be directly linked to specific clients included within the incident report. Financial entities

are not in a position to factor a calculation of the cost of non-compliance into their preliminary risk assessment; any cost calculation(s) due to contractual issues will be better understood over a longer period of time than the final report timeline of 20 days. Contractual costs do not inform the risk assessment of the specific incident and are not linked to how the incident was resolved, the root cause or the impact of the incident, rather, they depend on the service offered and the specific contractual arrangement with the individual client. We recommend that the data field is removed.

We would also like to raise our concern regarding the extensive set of data required to estimate and provide the amount of each cost & loss per subcategory, particularly in the section for the final report and the imposition of strict timelines on different types of institutions, considering variations in sector criticality.

Question 5:
Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.

Partially

Typo in the RTS on incident reporting:

On page 88 – row "14. Description of the significant cyber threat" – column "Instruction": the text "information on about the probability of materialisation of the significant cyber threat;" is duplicated. This needs to be addressed.

Question 6:
Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

Partially

A question arises regarding the scope of incident reporting requirements as they pertain to EU-based financial institutions with global operations. Specifically, the query seeks to clarify whether these institutions are obligated to disclose cybersecurity incidents and operational disruptions occurring in their subsidiaries located outside the EU, in jurisdictions not directly covered by DORA. This situation is particularly relevant for financial institutions that have a complex international presence, including operations in countries where DORA's regulatory framework does not apply directly.

ABBL's response to ESAs consultation on DORA Batch 2 Policy Mandate

Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents (JC 2023 68)

Date: 1 March 2024
EU Transparency register: 3505006282-58

Question 1:
Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

Partially

We would like to highlight the lack of detail in defining which costs should be included versus excluded in incidents. We would like to raise concern regarding the difficulty in obtaining certain information required, particularly regarding losses due to forgone revenues, which are described as sounding like a loss of opportunity.

Accounting and financial systems are not set-up the way to easily allocate the staff, communication, and replacement costs directly to a single or aggregated incidents of similar nature. Hence, finding links to direct or indirect costs determination is problematic adding potential costs for enabling such tracing (if possible). In addition, the materialisation of some costs and timeframes obligations are not aligned e.g. fees, legal counselling or advisory costs associated with the incident. Such procedures are usually taking more time making it hard to be part of the classification and to be included in the annual aggregate cost and loss report.

Therefore, we propose a more simplified criteria approach as an alternative solution:

Having economic impact criterion at high-level leaving flexibility to the institutions which costs and losses are relevant for an ITC-related incident. We suggest removing direct and indirect part and reword as suggested below:

- the economic impact, any relevant costs and losses incurred as a company consequence of the ICT-related incident.

We would also like to raise concerns on the cost estimation in the situation of a group where costs of ICT Incidents costs may be shared. For example, two entities of the same group report costs to their respective competent authorities would report the same cost liked to the same incident that would then be "duplicate" when aggregating incidents cost across Europe.

We would like to ask clarification by ESAs as to excluding costs occurring at the service provider (also considering the usual situation of ICT incidents occurring intragroup or at third-party).

We generally agree with the alignment of the reference period with accounting year.

Question 2:
Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

Partially

We would like to ask ESAs for more clarification regarding the complexity and linkage between operational risk management and accounting processes. We also suggest enhancing the reporting channels for more advanced communication and automation requirements.

Additionally, we would request to clarify whether an external validation of the report would be required.

Question 3:
Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

Partially

We would like to raise our concern as to the additional burden caused by reporting cost of each major ICT incident individually.

The estimation provided during the incident reporting period (i.e. time between incident detection and final report) and the one which will be delivered in the annual report have a possibility to change (because of later events for example). Hence, delivering the gross and net costs and losses of each major ICT Incident individually would pose an inappropriate additional burden for this added granularity.

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA Batch 2 Policy Mandate

Draft Regulatory Technical Standards specifying elements related to threat led penetration tests (JC 2023 72)

Date: 1 March 2024
EU Transparency register: 3505006282-58

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

Partially

Accordance with TIBER-EU: The financial sector supports 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 both an individual financial institution and third-party provider or for pooled tests, containing multiple financial institutions or third-party providers. The RTS on TLPT maintains the concept of these tests, per the Level 1 text, however, it does not provide further guidance concerning their operationalisation. Both forms of test represent significant complexity with material legal, operational, and practical challenges that have yet to become established norms within the financial or technology sectors. The financial entity, who would be accountable for administering both tests, would face significant risk if they were required by a TLPT authority to do a combined or pooled test. All stages of the TLPT explained within the RTS would not be met and the expected timelines do not reflect the complexity of either test. We believe that further guidance concerning TLPT with third parties or pooled tests is necessary before such tests could be completed in practice. However, we also do not believe it is appropriate for specific guidance to be built within the short period remaining for the finalisation of this RTS, or without industry consultation. We recommend that combined and pooled tests are not considered by TLPT authorities until comprehensive guidance is produced by TIBER-EU. Further comments concerning the complexity of tests is included within Question 10.

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 immature 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 with the TLPT, following a summary from the financial entity, outlining why a purple teaming exercise would yield little to no benefit.

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 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 therefore propose the following amendments:

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."

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 request that the TLPT authority waive the mandatory requirement to complete a purple team exercise."

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

Partially

We would suggest having greater clarity on the criteria to identify who falls under the TLPT to enable a period of preparation for this exercise. While making reference to the opt-in or opt-out option from the TLPT Authority, we are wondering how these decisions will be made. Being in scope of TLPT or not can have major impact on FE and its compliance obligations. Therefore, all FEs need clarity and transparency about whether or not they will be in scope.

Furthermore, we would like to highlight the point of FE belonging to a group, G-SII: the question of the proportionality applied to the Group entity that may not have the same risk profile.

Proportionality: While we welcome the inclusion of a proportionality principle, we note that the exclusion of only microenterprises creates the possibility for a very large number of financial entities to be required to complete TLPTs under DORA. While we support the criteria for inclusion given in Art 26(8) of DORA, we are concerned that the inclusion of a large number of firms would challenge the proposed frequency. We note the text of paragraph 11 of the RTS which signals that TLPT authorities will have flexibility in setting the frequency of TLPTs. We support this flexibility and caution against the rigid enforcement of a 3-year rotation. We further suggest that NCAs retain significant flexibility to reduce the number of firms in scope beyond what is given in paragraph 27. In particular, as discussed below, 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 and make the frequency proposed in the Level 1 text more achievable.

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 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.

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.

Partially

We are concerned that the approach to identifying financial entities may 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 the same ICT systems with central control and cybersecurity departments that administer their internal testing programs. A TLPT authority could identify an FE for inclusion based on a "specific feature" with the result that the exact same ICT systems and control procedures that have already been tested by another TLPT authority are subject to another TLPT. This will add no value for the FE and largely be a duplication for the TLPT authority wasting limited resources.

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.

A further factor, alongside the same ICT systems, that the TLPT authority should take into account is if the financial entity is using common testing, control, and cybersecurity teams 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 teams 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 Art. 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 the proposed TLPT. We recommend the following amendment to Art 2(2) and corresponding amendment to Art 12(3):

• *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.

Please see Q12 for further information.

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. 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.

Partially

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):

a. TLPT authorities shall consider requiring (to delete: "~~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 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.

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

Partially

We wish to take this space to reiterate the importance of a collaborative process between 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 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.

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.

Partially

If third parties are involved or tests are conducted jointly, it is unclear on how to manage the risk in the context of an intra-group arrangements. More details on the risk management process for TLPT when FE has dependencies with other entities are appreciated. If several entities of a group share the same system, ESAs guidance on risk management process is appreciated. Likewise, it is not clear

whether for entities that are part of a group, the test of all systems has to be conducted every 3 years. As an option: to use the same the TLPT service provider for several entities belonging to the same group.

Equally, for pooled testing, the impression is that no risk assessment process is mentioned for the standard TLPT, which means, there is no clarity on who will endorse the risk management and assess risks and who takes responsibility.

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

o *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.

Partially

We believe that using less qualified and less experienced testers and service providers will have an impact on the risk-based approach and the risk management process. Are there means for FE to challenge these testers?

Regarding references: Can we clarify what constitutes a good reference? Perhaps the quality is more important in providing assurance about the service provider, than having a minimum number of references. Internet markets in general suffer from the problem of untrustworthy reviews. What are the requirements to ensure that the service provider's references are reliable and appropriate?

Also, FEs need flexibility in case of being unable to engage a suitable testing provider in the time allocated. The absence of such flexibility could delay the TLPT and should be considered in the risk management process. There is no guarantee that this type of profiles will be continuously available in the market. The ideal approach would be to have dialogue with the TLPT Authority, and to consider alternative approaches, including the use of internal testers, when otherwise not allowed.

Alignment to TIBER EU procurement guidelines: As per the Level 1 DORA text, the financial sector supports the RTS's 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. We anticipate a significant rise in the cost associated with procuring such services which may adversely impact smaller financial

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

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 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.

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.

Partially

We would be in favour of a more flexibility in terms of the number of years of experience for external testers and threat intelligence providers. We are concerned that higher level of standards, at least in the first several years of DORA application, would lead to a situation of a deficit of such experts in the market, and this consequently would drive prices up for respective TLPT services in the context of the lack of supply. Certain financial institutions will not be able to find suitable TLPT experts when needed. This situation should be avoided.

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

Partially

The timeline for the TLPT authority to reply in a timely manner to the different phases is unclear.

The number of touchpoints for approval with the TLPT authority is potentially quite challenging. This could have an impact on the testing exercise, and lead to delays. If several member state authorities are involved, which one is responsible for what approvals?

Red teaming timeline: The RTS requires the active red teaming test to be a minimum of 12 weeks. The industry believes that greater flexibility should be built in to the timeframes provided in the RTS. In particular, we believe that a focus on outcomes and objectives should be primary when considering when to end a red team test. We also note that if the objectives have been achieved then elongating the red team test only services to extend operational risk and jeopardize the secrecy of the test. We therefore 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*

(to delete: "~~in any case shall at least be")~~ ***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 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 1) allowing the control team to have a greater independence of decision making and 2) holding further pre-emptive discussions with the FE on the conditions for such decision-making including example scenarios. Below we suggest amendments in specific areas designed to achieve this.

Leg ups: 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 Art. 8(2) that the red team test plan should include consideration of when leg ups are to be provided. However, past 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:

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*** *(to delete: "~~and the TLPT authority")~~.*

Detection: 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:

*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, (to delete: "~~in consultation with the testers and~~") without prejudice to paragraph 10, shall **take** (to delete: "~~propose and submit~~") measures **according to the conditions laid out in the red team test plan** allowing to continue the TLPT (to delete: "~~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.

Partially

DORA's requirement for pooled testing lacks 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 regulators have consulted on the inclusion of third-party providers within TLPT testing and ultimately decided against it owing to the significant legal, and security complications that are created. 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

a) **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 a impractically larger number of TPPs being included in the scope of the TLPT. Ensuring sufficient legal rights, confidentiality of sensitive information and security controls for such a broad test would not be feasible.
b) **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).
c) 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 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.
d) **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 uncertainly is likely to serve as a significant barrier to contractual agreements between the FE and various other parties, whether TPPs or other FEs.
e) **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.
f) **Scenarios and TIP report:** Annex III does not make clear whether the TI provider would be expected to apply paragraph 2 to any in-scope TPPs as well as the financial entity. Doing so would represent a material extension of the TIP work and would likely require renegotiation

of the TIP contract. This is another area where there is a risk of a circular series of approvals and changes between the FE, TIP/testers, TPP and the TLPT authority in a pooled test or TLPT with TPPs in scope.

Testing Phase

g) **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.

h) **Control team**: There is significant uncertainly about how a control team would manage a test in a pooled test or in a TLPT with multiple TPPs in scope. In either scenario, all firms involved may reasonably expect to be included in the control team. This could result in the control team becoming unmanageable in size and impact the ability for quick decision making or frequent contact with the TLPT authority. It is also likely that participating firms would seek to restrict sensitive information from other participants out of concern for security and competition law. At a minimum, 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

i) **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.

We would appreciate a clarification that pooled testing should be managed by several TLPT authorities. In practice, pooled testing may be complex, and this should be taken into consideration.

On page 13, it is mentioned: "the cooperation of TLPT authorities (Article 14(2)) and the attestation (Article 15(5))". However, there are no Article 14 and 15 in the RTS.

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.

Partially

Policy for the management of internal testers: The RTS Art. 11 requires several controls related to the use of internal testers. While we agree with the controls listed, they would not necessarily make sense if applied to the group-wide internal policy for the financial entity's red team operations, rather than only DORA TLPTs. We therefore suggest an amendment below to clarify that these requirements apply to conducting DORA TLPT and not as a general ICT risk management requirement on all FEs subject to DORA.

> 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**."

We believe the level of the qualification does not specify the criteria on the level of experience. It is not clear whether the requirements apply to both internal and external testers for certifications, years of experience, and number of conducted TLPT exercises.

Intragroup TLPT

> Banks within the EU are increasingly centralizing their cybersecurity operations, including in/out internet networks, at the group level, rather than managing these functions locally. This change in operational structure raises questions regarding the adherence to the TLPT obligations outlined in the current draft RTS. Specifically, there is a need for clarity on whether and to what extent banks can outsource their TLPT obligations to their parent group, especially when the management of their network infrastructure is also centralized at the group level.
>
> To address this concern, it is proposed that the ESAs consider incorporating the following provisions into the draft RTS:
>
> - Further clarification on Intragroup TLPT obligations: We would welcome more guidance on the conditions under which banks can conduct TLPT within the group. This guidance should detail the framework for such intragroup TLPT activities including standards for the coordination and execution of TLPT to ensure comprehensive coverage of all critical assets managed at the group level, while also respecting the regulatory requirements of each jurisdiction where the group operates.
> - Provisions for cross-border TLPT execution: As many banking groups operate across multiple jurisdictions, the RTS should facilitate cross-border TLPT execution, acknowledging the centralized management of network infrastructures and the need for consistent cybersecurity testing across all entities within the group.

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

Partially

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. The financial entity, in addition, should still be allowed to respond to

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

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 complication 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 and defensive teams that the financial entity utilises in common between its operations in multiple 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 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 testing 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.

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.

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's response to ESAs consultation on DORA Batch 2 Policy Mandate

JC 2023 69 - Draft regulatory technical standard on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), (b) and (d) of Regulation (EU) 2022/2554

Date: 1 March 2024

EU Transparency register: 3505006282-58

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

Partially

In general, we recommend establishing provisions within the RTS that allow entities to leverage group-level oversight mechanisms to meet the standards and requirements set forth by DORA without necessitating redundant assessments, thus promoting efficiency while maintaining operational resilience.

At this moment, it is not clear how information provided by financial entities will be shared, coordinated, and harmonised with subcontractors. Furthermore, how will supervisory authorities address any data asymmetry, and how will this situation affect financial entities' supervision.

Question 2:
Is the process to assess the completeness of opt-in application clear and understandable? (Article 2)

Question 3:
Is the list of information to be provided by CTPP to the LO that is necessary to carry out its duties clear and complete? Please, provide comments on information to be added or removed including the rationale (Article 3)

Question 4:
Do you agree with the content of Article 4 on remediation plan and progress reports?

Question 5:
Is the article on the structure and format of information provided by the CTPP appropriate and structured? (Article 5)

Partially

We would like to ask to which extent would the information provided by CTPP to Lead Overseers (or at least a subset) made available to Financial Entities using services from CTPPs. That would indeed enable (i) financial entities to use a single repository for collecting CTPP information (hence enabling a more efficient due diligence and monitoring/oversight and (ii) reduce the CTPP's effort to respond to their financial sector clients' due diligence or monitoring/oversight. It would not completely substitute the whole due diligence/monitoring process from financial entities but rather provide more efficiency. In particular, the information provided by CTPP required in Article 5, the list of sub-contractors required in Article 6 and recommendation of Lead Overseer from Article 7 would be highly relevant for FE.

Question 6:
Is the information to be provided by the CTPP to the LO complete, appropriate and structured? (Article 6 and Annex I)

Question 7:
Is Article 7 on competent authorities' assessment of the risks addressed in the recommendations of the LO clear?

Question 8:
Do you agree with the impact assessment and the main conclusions stemming from it?

Yes