Position Paper

European Commission Proposal for a Regulation on Digital Operational Resilience of the Financial Sector (DORA)

15 February 2021

Executive Summary

The Association for Financial Markets in Europe (AFME) supports the European Commission's (Commission) proposal ('the proposal') for a '**Regulation on Digital Operational Resilience in the Financial Sector' (DORA).** We believe that the aim of the proposal is a positive effort to harmonise the European financial regulatory framework and enhance the resilience and security of the financial sector. The proposal also provides an opportunity to enhance understanding and transparency between financial entities, regulators, and third-party providers; supporting the objectives of the EU digital finance agenda in promoting innovative and competitive financial services.

To achieve these objectives, we have summarised below our key considerations for the proposal,

- A risk-based approach should be adopted that aligns with the existing EBA Guidelines on ICT and Security Risk Management and Guidelines on Outsourcing Arrangements (e.g. 'EBA Guidelines'). This will increase regulatory harmonisation, and ensure financial entities are able to implement the requirements effectively, by providing the legal clarity needed to meet the objective of a digitally resilient financial sector. A risk-based approach will provide the flexibility needed for financial entities to allocate resources proportionately, where they are the most effective, and remain adaptive to an evolving risk and technology landscape.
- Definitions and terms in the proposal should be amended to be consistent with existing regional and global terminology (e.g. EBA Guidelines, FSB Cyber Lexicon, BCBS Principles for Operational Resilience). Inconsistent terminology will be difficult for financial entities to implement and lead to further regulatory complexity within the EU and cross-border.
- A period of 36 months should be provided for the implementation of the proposal once it enters into force. This is to allow for the significant number of Regulatory Technical Standards (RTS), mandated to European Supervisory Authorities (ESAs), that will be published within the first 12 months; currently the same period that financial entities will be expected to be compliant with the proposal.
- The requirement for financial entities to disclose major vulnerabilities should be removed due to the sensitivity and significant risk of cyber-attacks if this information was inadvertently exposed. Similarly, while we support efforts to increase information sharing and collaboration to prevent incidents, a more risk-based approach should be taken to reduce the reporting burden this will create for financial entities and supervisors, and the risk of sensitive data being too widely disseminated.
- Mutual recognition of Threat Lead Penetration Testing (TLPT) within the EU, and with other jurisdictions, should be added to the proposal and reference to the TIBER-EU framework. This will support the objective of developing a common pan-European approach to TLPT.
- Clarity should be provided in the recitals that financial entities would not fall under the definition and requirements of an ICT third party provider and that intra-group ICT providers are included in the definition of financial entities as outlined in the proposal.
- The limitations on the use of third-country third-party providers and sub-outsourcers should be removed. This is to prevent localisation and a loss of access to services which would impact the competitiveness of EU financial entities and cross-border activity.
- An objective of the Oversight Framework should be to reduce the burden placed on financial entities in relation to their obligations over Critical Third-Party Providers (CTPPs). Whilst we acknowledge that CTTPs will not be excluded from the risk mitigation policies of financial entities, the Oversight Framework should provide assurances for requirements such as outsourcing notifications and audits and inspections.
- Financial entities should be made aware of the recommendations of the Lead Overseer in relation to a CTPP, via the CTTP directly and ongoing discussions, to allow for appropriate risk assessments to be taken as needed.

- The requirements for financial entities to suspend, or terminate, a service or relationship with a CTPP should only be required as a last resort where Lead Overseer concerns cannot be addressed by alternative means, and sufficient time is allowed for any controlled and secure exit required.
- The Oversight Framework for CTTPs should be streamlined through a single ESA to increase the efficiency, and reduce fragmentation, in the implementation of the Oversight Framework. Further, sufficient investment will be needed to ensure that the Leader Overseer, and Oversight Forum participants, have the required skills and resources to perform these significant additional responsibilities in their role.

Our detailed assessment and recommendations are provided in the following paper and we look forward to continuing to support this important initiative as part of ongoing negotiations.

1. Chapter I: General Provisions

Subject matter (Article 1)

We recommend that the scope of the oversight framework is clarified regarding entities based outside of the EU and servicing EU financial services entities (Art.1.c). If these entities fall under the scope of the regulation this could create uncertainty and complexity for financial entities ongoing use of third-country providers and impact cross-border activity (by unintentionally leading to localisation of third-party use). We recommend further consideration is given to the potential unintended consequence which may limit access to, and the adoption of, new technologies and innovation within the EU.

Definitions (Article 3)

The definition of digital operational resilience (Art 3.1) is not consistent with existing global definitions such as the Basel Committee for Banking Supervision (BCBS)[1]. Global consistency for definitions and terms applicable to operational resilience will provide clarity and legal certainty for financial entities, particularly for those operating cross-border. Any divergence will increase the burden on cross-border financial entities who will be required to reconcile different interpretations to meet similar regulatory expectations in different jurisdictions. We recommend that the definition of digital operational resilience is consistent with the BCBS definition.

Several definitions are inconsistent in the proposal with globally recognised terms, such as in the FSB Cyber Lexicon[2]. These include Network and information system (Art. 3.2); Information asset (Art. 3.5); ICT-related incident (Art. 3.6); Cyber threat (Art. 3.8); Cyber-attack (Art. 3.9); Threat intelligence (Art. 3.10); Defence-in-depth (Art. 3.11); and Threat led penetration testing (Art. 3.13). We recommend that these definitions are amended to be consistent globally with the FSB Cyber Lexicon.

To ensure consistency with the existing EBA Guidelines on Outsourcing Arrangements, definitions such as 'ICT third-party service provider' (3.15), and 'ICT services' (3.16), should be aligned with the concept of outsourcing according to the EBA Guidelines[3]. This should also include the exceptions which would not be subject to these requirements, such as market information services, as outlined in the EBA Guidelines (paragraph 28).

The EBA Guidelines on Outsourcing Arrangements define factors that financial entities should consider when assessing whether an outsourcing arrangement is critical or important (EBA GLs, articles 29, 30, and 31). We recommend that the definition of 'critical or important functions' (Art. 3.17) should be aligned with the EBA Guidelines on Outsourcing so this consistency is maintained.

It is unclear if financial entities could be classified as ICT third parties under the proposal. This means financial entities could fall under the scope of the prudential/supervisory framework and proposed Oversight Framework (such as for intergroup arrangements). We recommend that financial entities cannot fall under the application or definition of an ICT third party provider in the proposal, and that intra-group ICT providers are included in the definition of financial entities. We recommend that clarity is provided in the recitals.

The definition for 'major ICT-related incident' (Art. 3.7) could result in excessive levels of reported incidents by financial entities. This is because the use of the word 'potential' in the definition would significantly increase the threshold for what is considered a major incident. We recommend that the definition is amended, substituting the word '*potential*' with '*likely to have a significant*', reducing the risk of financial entities over-reporting incidents.

The definition for 'management body' (Art. 3.22) would significantly increase the scope of what is identified as the management body by financial entities and diverge from current EU regulatory requirements. In the definition, the inclusion of '*or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation*' expands the scope of the management body beyond what is necessary or required, incorporating the board, CEO/COO's and all key function holders. We recommend that this part is removed from the definition to ensure it is

[1] Basel Committee for Banking Supervision 'Principles for operational resilience' (August 2020)

[2] FSB Cyber Lexicon (November 2018)

[3] https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

manageable and proportionate for financial entities, and remains consistent with existing EU regulatory requirements, such as CRD Directive 2013/36 (see (7) page 14).

2. Chapter II: ICT Risk Management

Governance and organisation (Article 4)

We believe it is more appropriate for financial entities to implement risk-based requirements for managing ICT, cyber and outsourcing risks. This is because a risk-based approach is focused on achieving specific outcomes providing flexibility and proportionality, and is more readily implementable by a wide range of financial entities. This approach allows financial entities to maintain the effectiveness of risk mitigating capabilities and adjust resource allocation efficiently to an evolving risk and technology landscape.

Several requirements throughout the proposal describe in detail *how* financial entities should achieve specific outcomes rather than *the* outcome (e.g. what we have identified as 'overly prescriptive'). This limits the ability of financial entities to choose an implementation that suits their unique circumstance, or unique risk to which they might be exposed. Further, it increases the risk of introducing requirements which could quickly become outdated.

Therefore, we believe that financial entities should continue to have flexibility for the definition, approval, and oversight of all arrangements related to the ICT risk management framework (Art. 4.2) as is appropriate with a risk-based approach. We recommend that the proposals are aligned with the appropriate language and risk-based approach taken in the EBA Guidelines on ICT and Security Risk Management and Guidelines on Outsourcing Arrangements.

Further, the need for the management body of a financial entity to define and approve specific risk type policies is overly prescriptive and limits financial entities ability to allocate responsibility to existing governance models. We recommend that a more risk-based approach is taken that provides the flexibility for financial entities to allocate responsibilities and perform these activities as appropriate to the risk and expertise required.

We believe that the scope of 'ICT Business Continuity policy' (Art. 4.2.d) should be defined in relation to existing Business Continuity Policies that already refer to Disaster Recovery Policies and Cyber Policies and are specific components of Business Continuity Plans (e.g., Disaster Recovery Plan, Cyber-Attack Plan).

The requirement for a financial entities management body to be '*duly informed* about *all* ICT-related incidents*'* (Art. 4.2.i) is not consistent with the EBA Guidelines on ICT and Security Risk Management and is overly prescriptive. We believe that financial entities should continue to have flexibility for ICT incident and problem management in line with EBA Guidelines (60.d.ii). We recommend that flexibility is maintained for financial entities to perform these activities and that the management body is '*informed on an ad-hoc basis*', in line with EBA Guidelines.

ICT risk management framework (Article 5)

It is not clear how the proposed ICT Risk Management Framework (Art 5.1) is intended to complement, or overlap, with the EBA Guidelines on ICT and Security Risk Management[4]. This creates regulatory uncertainty and will potentially duplicate requirements for financial entities as part of their cyber and ICT security risk management. The EBA Guidelines have only recently been adopted by Member States and sufficient time has not passed to fully assess the need for additional requirements to mitigate any gaps in the EBA Guidelines.

For example, the definition of an ICT Risk Management Framework (Art. 5.2, 5.5, 5.6) is not consistent with the definition of ICT and Security Risk Management Framework in the EBA Guidelines on ICT and Security Risk Management. The definition in this proposal is too broad (referring to "strategies, policies, procedures, ICT protocols and tools" for the entire information system of a financial entity) and does not clarify roles and responsibilities based on the three lines of defence model that is included in the EBA Guidelines. Further, several of the measures proposed, such as requirements on three lines of defence segregation (Art. 5.5) and frequencies of documentation review (Art. 5.6) are overly prescriptive. Additionally, terms such as 'impact tolerance' (Art. 5.9.b) are provided without any definition and clarity on the meaning of the term is required.

In addition, the need for an extensive range of additional governance and controls as part of the ICT Risk Management Framework (Art. 5.9) will lead to an additional administrative burden and increased inefficiencies for financial entities, providing limited added value to financial entities in terms of risk mitigation. For example, the ICT Risk Management Framework is required to contain an information security management system, digital resilience strategy, ICT business continuity plan, ICT disaster recovery plan, incident communication strategies, ICT reference architectures, mappings of ICT systems, and information security policy. Each must be documented and collated under a single IT risk management framework for each legal entity under a financial entity group structure.

We recommend that the proposal is amended so that the ICT Risk Management Framework is consistent with the EBA Guidelines. This will allow for the flexibility needed by financial entities in how the ICT Risk Management Framework is developed and implemented, leveraging existing and mature governance structures, processes, documentation, and controls. This will reduce the compliance burden and duplication with financial entities existing arrangements whilst providing benefit to smaller and medium sized entities.

[4] https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

The requirement whereby financial entities may delegate the task of verifying compliance with the ICT risk management requirements to intra-group or external undertakings, upon approval by Competent Authorities (CAs) (Art. 5.10), will have significant implications for centralised risk management and compliance functions. For intra-group delegation, we recommend that CA approval should not be required.

ICT systems and tools (Article 6)

We support regulators efforts to acknowledge the use of internationally recognised standards and industry leading practices on information security and ICT internal controls (Art. 6.2). To promote consistency across the financial sector and reduce regulatory fragmentation, financial entities from various jurisdictions along with other industry associations developed in 2018 the Cyber Risk Institute's (CRI)[5] Cybersecurity Profile ("Profile"). The Profile is a globally recognised, scalable and extensible assessment tool that financial entities of all types can use for internal and external (i.e., third-party) cyber risk management and as a mechanism to evidence compliance with various regulatory frameworks, globally.

We recommend EU policymakers acknowledge the Profile as an internationally recognized technical standard/industry leading practice on information security and ICT internal controls.

Identification (Article 7)

Mapping activities (Art. 7.4, 7.7.) within an ICT Risk Management Framework (such as ICT related business functions and risks) is an important process that supports resource assessments critical to service delivery. Financial entities already rely on mapping as part of Business Continuity Management (BCM), Recovery and Resolution Planning (RRP), and Disaster Recovery (DR) efforts. Further, several terms do not provide sufficient clarity on how to appropriately interpret and implement the requirements in line with current principles and risk-based practices. For example, how financial entities shall identify, classify, and adequately document all ICT-related business functions (Art. 7.1), and what constitutes a major change and an appropriate risk assessment (Art. 7.3). Mappings also contain highly sensitive information; therefore, appropriate safeguards should be in place to protect them.

We recommend that a more proportionate approach to mapping requirements is proposed to address these challenges. In addition, we recommend that flexibility is provided to financial entities to determine what would be an adequate level of mapping to meet the intention of the requirements, especially where it is more appropriate for financial entities to continue performing these activities within existing operational resilience objectives (and aligned to the mapping requirements under the EBA Guidelines on ICT and Security Risk Management).

Finally, we recommend that proportionality, and a risk-based approach, is provided regarding requirements for conducting specific ICT risk assessment on all legacy ICT systems (Art. 7.7). This requirement is not consistent with the EBA Guidelines on ICT and Security Risk Management; the EBA Guidelines do not specify the need to carry out risk assessments on all legacy systems, but that systems must be classified and assessed according to their criticality.

Protection and prevention (Article 8)

The requirements for ICT protection and prevention are at risk of becoming obsolete over time as new technologies emerge. Some terms, such as 'state of the art' (Art. 8.3), should be reconsidered as they do not provide clear expectations to financial entities. We recommend that flexibility is provided to financial entities when performing protection and prevention activities to not impede technology developments and adoption and ensure financial entities can adjust relevant controls as required.

The requirements to implement automated mechanisms to isolate affected information assets in case of cyber-attacks (Art. 8.4.b) and to include changes to software, hardware, firmware components, systems, and security changes as part of ICT change management (Art. 8.4.e), are overly prescriptive. We recommend that flexibility is maintained for financial entities when performing ICT change management activities in a risk-based approach, and that alignment is maintained with the EBA Guidelines on ICT and Security Risk Management (3.6.3).

Detection (Article 9)

The requirements for detection (Art. 9.1), such as mandating automatic alert mechanisms, are prescriptive and do not provide the flexibility required for financial entities to appropriately meet digital operational resiliency objectives as appropriate. We recommended that flexibility is allowed within the specific requirements on detection in how they are implemented.

Response and recovery (Article 10)

The requirement for financial entities to test ICT business continuity plans with ICT third-party service providers (Art. 10.4) should provide more proportionality and more closely align with the EBA Guidelines on ICT and Security Risk management (3.7.4. 87). This is because some ICT infrastructures span multiple regions and service centres (e.g., some cloud computing infrastructures are spread across multiple data centres). In such circumstances it would be extremely difficult, costly, and disruptive to test yearly the entire infrastructure. We recommend that this requirement is amended so that parts of the infrastructure can be tested at different stages over time, and that testing is proportionate based on different levels of risks. In addition, we recommend that for the requirements for response and recovery activities (Art. 10.2.a, 10.2.c, 10.5.a, 10.7,

[5] https://cyberriskinstitute.org/

10.9) are aligned to the EBA Guidelines on ICT Risk and Security Management to ensure financial entities can meet ICT business continuity objectives as part of overall Business Continuity Management.

Backup policies and recovery methods (Article 11)

The use of the term 'backup' (Art. 11.1) to solutions for extreme scenarios (e.g., disaster recovery) could create uncertainty and misunderstanding for financial entities. This is because 'Backup management' is usually considered as an ICT management process that is focused on recovering normal operations in case of data loss, or corruption, due to component failures, IT procedure, application failures, operative errors, intentional or unintentional misconduct. We recommend that clarity is provided on the intention of the term backup in the content of this proposal. Further, we recommend that further clarity is provided in regards to '*ICT systems that have an operating environment different from the main one, that is not directly connected with the latter*' (Art. 13.3). A requirement for financial entities to have replicated production environments on a stand-by basis, to be used only in case of a contingency event, would entail significant costs for financial entities and be overly prescriptive.

Further, it would be beneficial if flexibility was provided in how financial entities prepare for ICT capacity and continuity of service, if Business Continuity needs are met, as those may evolve or change over time (Art. 11.4). We recommend that flexibility is provided for financial entities in managing redundant ICT capacity as part of a continuous evaluation of their Business Continuity capabilities (e.g., Recovery Sites, Business Continuity Plans, ICT capabilities).

Finally, taking account the overall impact on market efficiency (Art. 11.6), we note that it may be overly complex and difficult for financial entities to assess such impacts due to the limited information available to financial entities to determine market-wide impacts. We believe it will be important for regulators and financial entities to collaborate and support sector wide assessments, or cross-sectoral assessments, which may span multiple financial entities and borders. Therefore, we recommend instead that financial entities take steps to minimise disruption to customers and the wider market.

Learning and evolving (Article 12)

Financial entities will be required to communicate changes to competent authorities following post ICT-related incident reviews after significant ICT disruptions of their core activities (Art 12.2). We recommend further clarity as to what information should be required (or not) for these communications.

Financial entities will also be required to map the evolution of ICT risks over time with a view to enhance their cyber maturity (Art 12.4). We have concerns that this requirement will be overly complex and lacks precision in what is meant by 'evolution'. We recommend that financial entities can perform the activities listed in a manner that is flexible and proportionate to different levels of risks. In addition, we recommend that the requirement for compulsory ICT security programs and training for staff (Art. 12.6) is amended to provide flexibility to financial entities to determine which employees would be required for such training.

Communication (Article 13)

Financial entities will be required to have in place communication plans enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate (Art 13.1). We recommend that the requirement to disclose major vulnerabilities is removed as financial entities' vulnerability data can provide a clear roadmap to threat actors on how to attack a firm. It is imperative the distribution of vulnerabilities is tightly controlled.

Further harmonisation of ICT risk management tools, methods, processes and policies (Article 14)

The requirements for developing draft technical standards (Art. 14.b, 14.c, 14.d), such as developing components of the controls of access management rights, are prescriptive and do not provide the flexibility required for financial entities to appropriately meet ICT security risk management in line with EBA Guidelines. We recommended that specific requirements are amended to allow flexibility in how they will be developed in Regulatory Technical Standards.

3. Chapter III: ICT Related Incidents: Management, Classification and Reporting

ICT-related incident management process (Article 15)

Currently, within the EU, a number of intra-sector and cross-sector EU legislation and provisions set out different timeframes, taxonomies and thresholds for incident reporting (e.g., the GDPR, the eIDAS Regulation, the NIS directive, the ECB SSM). A fully harmonized cyber incident reporting regime, across all EU legislation, would provide significant benefit and efficiencies to financial entities and regulators.

The Financial Stability Board (FSB) published a toolkit on Cyber Incident Response and Recovery (CIRR)[6] in October 2020. The toolkit provides best practice for incident reporting as part of cyber incident response and recovery.

It is unclear how the ICT-related incident management process proposed complements or overlaps with the FSB standard global approach. We recommended that the process is aligned with this global standard to reduce regulatory uncertainty and the regulatory burden for cyber incident responses for financial entities; especially those operating cross-border. This

[6] FSB 'Effective Practices for Cyber Incident Response and Recovery: Final report' (October 2020)

will ensure financial entities are able to allocate resources where they are most effective, thus meeting the objective of a more digitally resilient financial sector.

Classification of ICT-related incidents (Article 16)

Regulators and financial entities would benefit from collaboration to develop a standardised and effective implementation for ICT-related incident criteria. For instance:

- How to assess reputational damage (Art. 16.1.a),
- When to consider that downtime has started (Art. 16.1.b),
- Whether geographical spread should include EU Member States, or European countries or other jurisdictions with critical operations (Art. 16.1.c),
- How severity (Art 16.1.1) and criticality (Art. 16.1.f) are defined, and
- How to determine economic impact (Art. 16.1.g).

Broad and varied regulatory incident reporting requirements, such as thresholds, could undermine the intent of reporting, which is to quickly identify threats and mitigate systemic risks. This can unintentionally inhibit digital resilience if financial entities over-notify incidents, including false positives, to meet the broad thresholds. This would make it more difficult to identify major incidents that need to be addressed and increase inefficiencies. We recommend that the criteria for incident classification is developed jointly with industry input, and that it is aligned with the FSB toolkit for CIRR.

Reporting of major ICT-related incidents (Article 17)

We welcome that the proposal provides flexibility to financial entities regarding the timing of reporting, and the expected harmonisation of reporting templates (Art. 17.1, 17.2, 17.3). However, detailed ICT-related incident reporting requirements risk diverting financial entities resources from incident management. Also, financial entities may have to provide incomplete information to satisfy prescriptive reporting timeframes. We recommend that reportable incidents should be limited to those incidents determined to have an impact (versus potential impact) which is consistent with existing requirements (such as GDPR). Further, we recommend that the timeframe for reporting should start from when a financial entity determines an impact to be likely, and not from when the incident took place.

We also note that the EBA and ECB have recently consulted on incident reporting under PSD2 in which they propose to raise the threshold for incidents reported explicitly to '*reduce the number of operational incidents that are required to be reported*'. In that consultation they remark that '*a large number of reported operational incidents appear to have a very low impact on the institution, with most of them related to failure of less significant tasks and single processes*.' We believe this analysis from the EBA and ECB should be taken into account in the on-going discussions on DORA to ensure an appropriate threshold and timeframe is adopted. We welcome that the ESAs be given the role of defining incidents to ensure reporting requirements remain flexible and in line with other incident reporting requirements currently under consideration (PSD2, NIS directive), as well as other RTS that the ESAs will produce, namely Art. 16.2a.

We support efforts to increase information sharing between public sector authorities and reduce the need for financial entities to report to multiple stakeholders when a major incident takes place (Art. 17.5). However, because reporting on major incidents contains sensitive data, we recommend a considered approach is taken on how incident reporting information is shared between stakeholders. Given the intention in the proposal to share summaries, it will be important that necessary safeguards are put in place to prevent confusion or misunderstanding from authorities when receiving reports second hand.

Harmonisation of reporting content and templates (Article 18)

We support the proposal to harmonise incident reporting templates across regulations, industry sectors, and European Member States (Art 18.1.a, 18.1.b). We also support the need to define a single standard reporting for all competent authorities applicable to ICT and security incidents.

Centralisation of reporting of major ICT-related incidents (Article 19)

We support the establishment of a single EU-hub for major ICT-related incident reporting (Art 19.1). A single hub for incident reporting, if appropriately designed and implemented, could provide significant benefits to financial entities and regulators by increasing the efficiency of incident reporting. This could be achieved in stages, initially establishing a central reporting and coordination hub at the Member State level with then a rolling-up into an EU hub (where consistency of reporting methods would be essential). However, as a single source of information, we recommend EU regulators carefully consider the potential risk for the single EU-hub to become the target of attacks. We would welcome the opportunity to input to this initiative and ensure the EU-hub is implemented to meet the intended outcomes.

4. Chapter IV: Digital Operational Resilience Testing

General requirements for the performance of digital operational resilience testing (Article 21)

A common pan-European Threat Lead Penetration Testing (TLPT) regime across the EU is welcomed as it will increase efficiency and reduce fragmentation. However, we note that requirements fostering mutual recognition of TLPT tests within

the EU, and outside of the EU, as well as reference to TIBER-EU, have not been incorporated in the proposal. We recommend that mutual recognition of Threat Lead Penetration Testing (TLPT) within the EU, and with other jurisdictions, is added to the proposal and reference to the TIBER-EU framework.

The proposal also places a strong emphasis on testing as a means to enhance a financial entity's digital resilience. While beneficial, testing is only one capability that financial entities use which must be balanced against inherent complexity, risks and costs. We believe it will also be important to incorporate enhanced continuous monitoring to avoid over-reliance on testing. We note that ENISA has allowed for this possibility in the recent proposal for an EU Cloud Security Certification, (e.g. continuous monitoring tools may be a core part of demonstrating resilience). We recommend that the proposal allows for developments in testing capabilities and approaches which can continue to satisfy the requirements in a more effective and secure manner over time.

We welcome the provision that financial entities should ensure that tests are undertaken by independent parties, whether internal or external (Art. 21.3). Flexibility will allow financial entities to prioritise testing efforts where they are most needed in a risk-based approach. We believe this should be the case for TLPT as well as other forms of testing.

However, the requirement to test all critical ICT systems and applications yearly is not practical and should be reconsidered (Art. 21.6). The requirement should include additional text allowing financial entities to follow a risk-based approach to ensure critical ICT systems and applications are tested regularly.

Testing of ICT tools and systems (Article 22)

We believe that the requirement to perform vulnerability assessments for all existing or new services supporting critical functions, rather than only those services that are themselves deemed critical, would be impractical and that proportionality is required (Art. 22.2).

It is unclear whether the expectation of DORA is that a firm will perform all of the testing methods listed in Art. 22.1 for each system tested in Art. 21.6. It is our view that this would neither be proportionate to the risk nor possible. We recommend that flexibility is provided to allow financial entities to use a risk-based approach towards the performance and requirement for the testing activities listed (Art 22.1).

Advanced testing of ICT tools, systems and processes based on threat led penetration testing (Article 23)

Testing live production systems should not be required if a financial entities' development and testing environments mirror that of production. Testing of all critical functions (Art. 23.2) would provide limited benefit for financial entities with shared infrastructure and consistent control frameworks, as it would be duplicative and unnecessarily increase costs and testing durations. We recommend that the proposals instead embed responsible behaviour as part of testing requirements so that due consideration is given to the impact of tests on financial entities resources, security, and potential for disruption. We recommend the text clarify that tests should be scoped from within the range of critical functions and services.

Further, we caution against any proposals that prescribe the frequency and requirement to test on live systems. This is because the testing of live systems requires due consideration for financial entities given the impact on resources and security, and the potential for disruption (especially when a financial entity's development and testing environments mirror that of production).

We also believe ICT third-party service providers (Art. 23.2) should not be included in the remit of threat lead penetration testing. Given ICT third-party providers may service several clients, significant duplication of testing would result from this requirement and could create significant risks for the provider of ICT services and the clients they service. We recommend that alternative processes should be considered, such as centralised independent third-party testing by certified testers (similar to existing CBEST practices).

The criteria used for determining which financial entities would be subject to carrying advanced testing by means of threat led penetration testing (Art. 23.1) is not defined, creating legal uncertainty. We recommend that the criteria used (Art. 23.4.a) take into account the criticality of the financial entity, not just its size. Finally, the reference to '*intelligence-based penetration tests*' (Art. 23.4) should be amended to 'threat-led penetration tests', to align with the provisions. If a different form of testing is meant, we recommend this be clarified and sufficient time be provided to financial entities to consider potential impacts.

Requirements for testers (Article 24)

Financial entities may have their own in-house testing team that is familiar with the financial entities environment or may use external testing providers. Mandating a specific approach for external testing providers (Art. 24.2, Art. 23.3) would place unnecessary financial burden on financial entities due to the scarcity and costs associated with third party providers thereby diverting resources from other security activities. To ensure the independence and objectivity of a financial entities-led test, financial entities should have a formal governance structure under which to conduct testing that includes defined testing standards and procedures, clear roles and responsibilities of the different teams involved, and rules of engagement, all of which may be reviewed with relevant authorities. We caution any requirement to mandate the outsourcing of testing to external testers and that financial entities continue to have the flexibility required to select the most appropriate testing provider whether internal or external.

5. Chapter V: Management of ICT Third-Party Risk

5.1. Section I: Key Principles for a sound management of ICT Third Party Risk

General principles (Article 25)

We support harmonised outsourcing and third-party risk management requirements applicable to financial entities and unregulated critical third parties, in line with EBA Guidelines. This will provide legal clarity, reduce fragmentation, promote financial stability, and increase regulatory efficiency for financial entities operating cross-border.

Financial entities are currently expected to meet the EBA Guidelines on Outsourcing Arrangements[7] as part of their third-party and outsourcing risk management. Insufficient time has passed since the Guidelines have been adopted by Member States to assess whether any gaps need to be mitigated, creating legal uncertainty. It would be beneficial as part of the general principles to build on the EBA Guidelines to further implement a harmonised approach to third-party risk and outsourcing across the EU.

Currently, it is unclear how the proposed third-party risk management framework (Art. 25.3, 25.4) complements or overlaps with the EBA Guidelines on Outsourcing Arrangements, which creates legal uncertainty and may potentially increase the regulatory burden on financial entities. We welcome further clarity on how the proposed third-party risk management framework will align with the EBA Guidelines (inclusive of the Outsourcing Register). We recommend the proposal scope, definitions, terminology and requirements align with the EBA Guidelines, to increase harmonisation across EU Member States and reduce complexity for financial entities. Currently this proposal's scope expands beyond outsourcing to cover all ICT services. We recommend that the proposal focuses only on critical or important activity (e.g. critical outsourced ICT activity) and provides greater proportionality, and flexibility, for financial entities to meet the requirements in a risk-based approach.

We would also welcome further clarity on how the proposed third-party risk management framework will be applied in the principle of proportionality (Art. 25.2), particularly for intra-group outsourcing arrangements. For example, some requirements specifically mention a risk-based approach (Art. 25.7), while others do not (e.g., 25.5; 25.8; 26.1; 26.2; 27.2). We recommend that the principle of proportionality is extended to all requirements so that a risk-based approach is adopted throughout the proposal. Further, the requirements do not establish a distinction for intra-group outsourcing arrangements (for example, exit plans would be needed for all outsourcing arrangements even if the group owns the provider). It is also unclear if financial entities could be classified as ICT third parties under the proposal. This means financial entities could fall under the scope of the prudential/supervisory framework and proposed Oversight Framework (such as for intergroup arrangements). We recommend that financial entities cannot fall under the application or definition of an ICT third party provider in the proposal and that intra-group ICT providers are included in the definition of financial entities. We recommend that clarity is provided in the recitals.

Requirements on multi-vendor strategies (Art. 5.9.g, 25.3, 25.4, 25.7, 25.8, 25.9*)* must not inadvertently impact the ability for a financial entity to manage outsourcing risk (e.g., through an integrated control framework to manage risks consistently), oversight obligations, enhance its resilience capabilities and adopt new technologies. Most large financial entities already use multi-vendor strategies, where necessary or appropriate, to mitigate third party risk as part of their own risk management procedures. When applied at a legal entity level, such rules could have unforeseen consequences that both challenge the global operating models of cross-border financial entities and increase operational risks. We recommend that this requirement is not mandated, and the use of multi-vendor strategies remains a risk-based and business decision of financial entities.

The requirement for financial entities to maintain a Register of Information in relation to all contractual arrangements on the use of ICT services, provided by ICT third-party service providers (Art. 25.4), is broader than the current requirements under the EBA Guidelines on Outsourcing Arrangements. This increase in scope and complexity, places additional compliance burden for financial entities. We recommend that it is more appropriate for financial entities to continue managing the activities listed for critical outsourced ICT activities, rather than all ICT services, and that flexibility is provided to allow a risk-based approach to those arrangements not classed as critical or important.

There is no commonly understood definition of '*latest information security standards*' (Art. 25.6) and therefore it would be difficult for financial entities to assess or enforce contractually. The objective of the requirement should be to ensure that ICT TPPs meet standards of security that are appropriate to the risk. We recommend that the wording '*latest information security standards*' is removed, or a clarifying statement added, referring to 'standards applicable to the industry'.

We are concerned that contractual arrangements between financial entities and ICT third-party service providers are terminated under certain conditions (Art. 25.8). This may create operational risk and can have unintended consequences for other group entities or reliant parties, including market uncertainty. We recommend that this requirement is aligned with the EBA Guidelines on Outsourcing Arrangements in particular that '*outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate the arrangement, in accordance with applicable law*' (13.4.98) for consistency and harmonisation with existing approaches. The requirements for financial entities to suspend, or terminate, a service or relationship with a CTPP should only be required as a last resort where Lead Overseer concerns cannot be addressed by alternative means to mitigate risks. For instance, it may be useful to consider a mechanism whereby CTTPs could explain how they are expected to meet recommendations made, before enforcement measures are considered.

[7] EBA 'Guidelines on Outsourcing Arrangements' (February 2019)

We recommend sufficient time is allowed for any controlled and secure exit required for impacted financial entities, as the risks of an immediate termination may in certain circumstances significantly outweigh any benefits.

Finally, a detailed and documented risk assessment of all ICT third party providers, including subcontractors and country risks, as well as a documented exit strategy, would be excessively burdensome for financial entities to implement (Art. 25.9). We recommend limiting this approach only to critical ICT service providers. A common taxonomy and understanding of ICT critical service providers would also be beneficial to financial entities.

Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements (Article 26)

We recommend that the identification and assessment of appropriate ICT third party providers remains driven by financial entities (Art. 26.1.a). For instance, it should be for financial entities to determine what is '*not easily substitutable*'. This will provide sufficient flexibility to financial entities to perform adequate risk assessments based on existing capabilities. Further, we recommend that '*multiple contractual arrangements*' should only require a concentration risk assessment where those arrangements are for critical and important functions.

Key contractual provisions (Article 27)

We are concerned that key contractual provisions apply to all contractual arrangements for ICT services and not just those in respect of critical or important functions (Art. 27.2). Given there is no materiality threshold for the definition of '*ICT services*' this could extend the application of these requirements well beyond the equivalent requirements in the EBA Guidelines on Outsourcing Arrangements. Equally, we note that a full contract, including service level agreements, documented in one written document, is potentially impractical for some outsourcing arrangements (Art. 27.1) and should be reconsidered to provide proportionality and flexibility to financial entities. We recommend that the key contractual provisions are aligned to the EBA Guidelines on Outsourcing Arrangements and focused on critical or important ICT services, and a risk-based approach is applied for non-critical or important ICT services.

Regarding exercising contractual access, inspection, and audit rights over the ICT third-party service provider (Art. 27.2.h), we recommend that consideration is given on the potential for disruption, and options for pooled audits can continue to be used (such as those in the EBA Guidelines on Outsourcing Arrangements).

Regarding contractual termination rights in accordance with competent authorities' expectations (Art. 27.2.j), we recommend that the proposal is streamlined through a single European Supervisory Authority (ESA) as a Lead Overseer in the proposed Oversight Framework. This will prevent fragmentation by National Competent Authorities (NCAs) in how termination rights may be exercised and provide greater harmonisation across the EU.

Finally, we are supportive of standard contractual clauses where they can support financial entities and providers with compliance with regulatory and supervisory requirements (Art. 27.3). This can also benefit both financial entities and providers in the negotiation process where required.

5.2. Section II: Oversight framework of critical ICT third-party service providers

Designation of critical ICT third-party service providers (Article 28)

We support a single EU approach and forum for identifying concentration risk which may bring consistency and efficiency of reporting and provide increased assurances for financial entities use of critical ICT third-party providers (Art. 28.1). We would also like to note our support for the designation of a single ESA as Lead Overseer, to increase the efficiency and reduce fragmentation.

The criteria for selecting the Lead Overseer (Art. 28.1) is based on the composition of CTPP clients rather than the service they provide. This raises the question of whether the Lead Overseer would change, to reflect changes in composition of CTPP clients. We recommend that an alternative approach would be to assign the Lead Overseer based on expertise and familiarity with the business model of a CTPP.

Further, we believe the criteria for determining CTTPs (Art 28.2.a, b, c, d, e, f) is too broad and could result in capturing too many third-party providers. This would be detrimental to the objective of identifying and mitigating systemic risk within the EU financial sector. We recommend a risk-based approach which considers both the provider and the nature of the service provided.

Also, it is unclear if financial entities could be classified as ICT third parties under the proposal. This means financial entities could fall under the scope of the prudential/supervisory framework and proposed oversight regime. We recommend clarity is provided in the recitals that financial entities, including intra-groups (e.g., where the group provides ICT services to affiliates), do not fall under the application or definition of an ICT third party provider in the proposal and that intra-group ICT providers are included in the definition of financial entities.

Designation of an ICT TTP as critical may affect the relationship between a financial entity and its ICT TTP. We recommend the text be amended to recognise that financial entities will need time to adjust internal processes and potentially contractual relationships with ICT TPPs designated as critical (Article 28.6). We recommend a period of 12 months should be allowed between the oversight forum determining that an ICT TPP is critical and that designation coming into force.

The requirement for competent authorities to transmit on a yearly and aggregated basis the reports referred to in Art. 25.4 to the Oversight Forum, could include sensitive information about financial entities (Article 28.7). We recommend that the annual reports are anonymised to ensure no sensitive information regarding financial entities is exposed, as sensitive data can provide a roadmap to threat actors on how to attack a firm. It is imperative the distribution of sensitive information is tightly controlled.

We also believe that the requirement limiting financial entities from making use of an ICT third-party service provider established in a third country that would be designated as critical (Art 28.9) could pose significant challenges to financial entities and the EU financial sector. This requirement as written would create incompatibility with cross-border operating models and group structures employed by many EU financial entities (e.g., inter-affiliate services), and require duplicative governance structures under existing outsourcing programs. This could make it more difficult for financial entities to operate cross-border if it unintentionally leads to localisation of third-party use and reduces the competitiveness of EU financial services more broadly. Further, we believe that maintaining the EU's attractiveness and competitiveness as a global hub for financial services, and innovative technologies, is essential for realising key European projects such as the EU Single Market and Capital Markets Union (CMU). We recommended that this requirement is removed. We believe that the EBA guidelines on outsourcing already provide a robust framework for the sound management of third-country third-party providers, whilst meeting supervisory expectations, without limiting use by financial entities.

Tasks of the Lead Overseer (Article 30)

We believe that the oversight framework could alleviate some of the burden placed on financial entities, such as requirements for performing outsourcing notifications, and audits and inspections, over CTPPs. CTPPs would not be excluded from the risk mitigation policies of financial entities, but inspection and audit obligations could be executed directly by the Lead Overseer (Art. 30.2), in view of meeting regulatory requirements. We recommend that non-objection practices for critical outsourcing to CTPPs subject to oversight should be removed, or reduced, as a requirement for financial entities as part of this proposal.

We believe it is not necessary for CTPPs to make financial institutions aware of all ICT-related incidents as the majority may be of no relevance (Art 30.2.e). We recommend that this is amended to focus on 'major' ICT-related incidents.

Further, we recommend that assessments on '*data portability, application of portability and interoperability*' for the provision of critical services should be led by financial entities rather than the Lead Overseer (Article 30.f). For instance, it should be for the financial entity to assess service portability based upon service details owned by the financial entity, and this could be complemented by Lead Overseer assessments on portability capabilities of CTTPs. This will provide sufficient flexibility to financial entities to perform adequate assessments based on existing capabilities.

Powers of the Lead Overseer (Article 31)

CTPPs should have an opportunity to discuss, and if needed appeal, recommendations of the Lead Overseer to allow sufficient time to assess potential viable options and understand wider impacts (Art. 31.9) before imposing enforcement measures such as penalty regimes. For instance, allowing for due diligence to ensure that the recommendations provided by the Lead Overseer will not increase the risk on financial entities. This will also allow for an appropriate level of flexibility and proportionality in the implementation of the recommendations prior to potential enforcement. We recommend financial entities are made aware and involved in discussions on the recommendations between the Lead Overseer and CTPPs, via the CTTP directly where these would likely affect the relationship between CTTPs and financial entities (such as existing contractual arrangements). This will also satisfy the need for competent authorities to monitor whether financial entities take into account risks identified in the recommendations addressed to CTPPs by the Lead Overseer (Art. 37.2).

We believe that the requirement limiting financial entities from making use of a subcontracting ICT third-party service provider established in a third country that would be designated as critical (Article 31.1.d.iv) could pose significant challenges to financial entities and the EU financial sector. This requirement as written would create incompatibility with cross-border operating models and group structures employed by many EU financial entities (e.g., inter-affiliate services), and require duplicative governance structures under existing outsourcing programs. This could make it more difficult for financial entities to operate cross-border if it unintentionally leads to localisation of third-party use and reduces the competitiveness of EU financial services more broadly. Further, we believe that maintaining the EU's attractiveness and competitiveness as a global hub for financial services, and innovative technologies, is essential for realising key European projects such as the EU Single Market and Capital Markets Union (CMU). Also, the requirement is duplicative of controls required by financial entities already provided in the proposal (Art. 26.2, 27.2.a, 31.1.iii). We recommended that this requirement is removed.

Request for information (Article 32)

We acknowledge the need for the Lead Overseer to request information that is required for completing relevant risk assessments under the oversight framework (Art. 32.1). However, appropriate safeguards will be needed to ensure the transfer and use of information which may contain commercial or confidential data of CTPP clients. We recommend that all information requests from the Lead Overseer to a CTPP for data related to financial entities (such as client data, commercial data, or data regarding the conduct of their business) should be made directly to financial entities, and not the CTPP, within the oversight forum. In particular, we do not believe it is appropriate for the Lead Overseer to be able to gain information related to the financial entity through 'simple request'. Financial entities typically have contractual rights to be notified by

their ICT TPP of information requested through formal. Therefore, to help protect EU financial entities confidentiality all such requests to CTPP's should use the mechanism in Art. 32.3 and not 'simple request'.

Ongoing Oversight (Article 35)

We believe that it is important financial entities are made aware of any CTPP risks identified by the Lead Overseer so that any appropriate changes can be made (such as to contractual arrangements or security measures) (Art. 35.5). We recommend that impacted financial entities are informed of risks via the oversight forum.

Follow-up by competent authorities (Article 37)

There is a risk of fragmentation if divergent approaches are implemented in each Member State, where National Competent Authorities may have their own approach on how to implement the findings of the Lead Overseer for designated CTPPs. Duplication, or a lack of clarity, in roles and supervisory powers will limit the effectiveness of a single EU forum. This could impact financial entities operating cross-border and ensuring a level-playing field in the financial services sector. We recommend that the powers of the Lead Overseer are streamlined through a single ESA, and the structure and participants of the Oversight Forum (Art. 29), is focused on simplifying the current obligations and reporting that is required by financial entities to both regional and national authorities (preventing separate national oversight processes and powers where they are duplicative to this proposal and the role of the Lead Overseer).

We are cautious of the provision for competent authorities to require financial entities to temporarily suspend or terminate, either in part or completely, the use or deployment of a service provided by the CTPP until the risks identified in the recommendations have been addressed (Art 37.3). Requirements for any immediate termination with a CTPP could impact financial entities business and commercial decision-making (deterring investments in the EU) and potentially impact business continuity and financial stability. We recommend that any termination should be carefully considered as a last resort option, where alternative measures are fully considered within the Oversight Framework, and that sufficient time and notice to financial entities is provided for executing safe transitions if required. Further, we recommend that it should be for the oversight forum to determine any termination required to ensure consistency across the EU and NCAs and avoid fragmentation in how this regulatory measure is implemented. We recommend that in taking this decision, authorities also consider whether suspension or termination introduces operational risks for critical third-party provider customers. We note that the degree of provider substitutability and the lack of alternative providers, would make porting to another provider difficult for financial entities.

International cooperation (Article 39)

We believe that to effectively mitigate critical third-party risks, within the financial sector and beyond, regulators would benefit from collaboration with financial entities and international partners to provide guidance on how the framework should be effectively implemented. This would preserve market integrity and competitiveness in the EU. We welcome further clarity on how mitigation of critical third-party risks in the financial sector will align with international bodies and forums as part of this proposal (e.g., FSB, BCBS).

6. Chapter VI: On Information Sharing Arrangements

Information-sharing arrangements on cyber threat information and intelligence (Article 40)

To increase the effective identification and mitigation of threats, financial entities benefit from voluntary information sharing, in a way that does not limit the qualitative input of financial entities in trusted information sharing networks (Art. 40.1). For example, providing an explicit basis to allow the exchange of personal information (such as IP addresses) would allow financial entities to enhance their defensive capabilities, better identify threats, and reduce the risk of contagion between financial entities. Also, we believe mandatory participation could erode the trusted relationship that exists between voluntary participants which would undermine overall digital resilience. We recommend participation in information sharing networks remains voluntary and that clarity is provided on the ability for financial entities to exchange personal information, to mitigate cyber threats.

Where public authorities would be involved, we recommend regulators consider that the sharing of cyber threats and incidents could present challenges for financial entities due to the confidential/sensitive nature of the information. The aim of information sharing should be to establish trust and therefore appropriate segregation should be established between the different functions a regulator may fulfil. We recommend that authorities in their capacity as supervisors should not have access to industry information sharing networks, which could significantly reduce the benefits of information sharing and change the nature of these trusted networks (financial entities may be scrutinised on the basis of the information shared (Art. 40.3)).

Similarly, Article 40.3 provides that financial entities shall notify competent authorities of their participation in the information-sharing arrangements. We recommend that this provision is removed as financial entities could be scrutinised on this basis which in turn could alter the perception of participation as voluntary and therefore undermine the trust necessary for such forums to be successful.

7. Chapter IX: Transitional and final provisions

Entry into force and application (Article 56)

The current expectation for implementation is not realistic and should be revised. The proposal includes several Regulatory Technical Standards (RTS) mandated to ESAs to be published a year after the proposal enters into force. As all the RTS under this proposal will require significant work from the ESAs, and will potentially be complex and technical, we do not believe it is desirable to accelerate the timeline for their delivery. Some RTS may require organisational and technology changes from financial entities. This is also at the same time financial entities should be expected to be compliant with the proposal. To account for this additional complexity, we recommend a more considerate timeline, providing 36 months to financial entities.