AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Digital Operations Resilience Act (DORA)

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

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

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Digital Operational Resilience Act - priority areas

The Digital Operational Resilience Act (DORA) represents a step towards a harmonised EU framework for digital resilience in financial operations, making the system both robust. future-proof and ready for the challenges of digitisation.

There is an urgent need for a coordinated international approach to Information and Communications Technology (ICT) risk management. The issues addressed in our previous positions[1] include recommendations from the banking sector, the cloud and software industry, as well as a data aggregator perspective of the framework.

Further to the amendments to the European Parliament's proposal for DORA, there are areas for which the current amendments are welcome, but also aspects in the proposed amendments where there should be further refinement. In addition to the previously outlined feedback on the amendments, the following recommendations provide additional perspectives as the Digital Operational Resilience Act moves into the trilogue negotiations.

Third-country issues

Issue/Concern	**Definition of 'ICT third-party service provider/sub-contractor established in a third country' (article 3[19])**
Preferred text	Original Commission (COM) text
Explanation	Due to changes to the definition in both the European Parliament (EP) and Council drafts, entities of the ICT provider located in third countries would be directly regulated by DORA. The change in both the EP and Council draft do not take into account the global nature of international ICT providers that maintain businesses in the EU. The Commission draft considers sufficient EU entities as a precondition for not falling in the scope of the definition of 'ICT third-party service providers established in a third country', under the definitions provided in both the EP and Council texts. However, these third-country entities are directly regulated under DORA, which unnecessarily extends the scope.

Issue/Concern	**Designation of critical ICT third-party providers (article 28[8a], [9])**
Preferred text	Council
Explanation	The Parliament introduces the article 28(8a), which establishes the possibility for the third country entities of an ICT provider to be designated as a critical ICT third-party provider. This would be an expansion of the scope that the Commission did not intend for. The Council does not make any similar suggestions. We, therefore, support the Council's draft. Additionally, we support the Council text in article 28(9) as it allows EU financial entities to contract with third-country ICT third-party providers if they also have an establishment within the EU. Additionally, the Council draft does not require third-

[1] Reaction to the amendments (July 2021) http://www.amchameu.eu/position-papers/dora-reaction-amendments and AmCham EU's original paper (March 2021) http://www.amchameu.eu/position-papers/digital-operational-resilience-act-dora

	country providers to include provisions like in article 27(2b) of the European Parliament's draft in their contracts.

Issue/Concern	**On-site audits of sites located in third countries by the Lead Overseer (article 34[1])**
Preferred text	Council text or original COM text
Explanation	The EP draft, contrary to the Council draft, explicitly allows for on-site audits of sites located in third countries by the Lead Overseer. While we acknowledge that the legislator wishes to ensure the Lead Overseer's jurisdictional powers over non-EU ICT providers, we consider that the accumulation of article 28(9), the contractual guarantees in article 27(2B), EP draft, and article 34(1), EP draft, is exaggerated and that the combination of these articles goes beyond what is necessary to ensure the jurisdictional reach. Hence, we recommend better dimensioning those provisions by deleting the superfluous requirements. The EC or Council draft should be supported, as the EP draft allows for on-site audits of sites in third countries. This is in line with the fact that the Council draft does not submit third country ICT third-party service providers to the oversight of a Lead Overseer (see article 28[9] above).

Timing

Issue/Concern	**Allowing sufficient time for compliance with DORA**
Preferred text	NA
Explanation	We do not believe the current timing expectations for implementation are sufficient. 24 months is not sufficient time to allow financial entities to make the many organisational and technological changes necessary to comply. More time is required as a result of the complexity and scale of the requirements in DORA, and to the limited time between compliance and publication of the many level-2 Regulatory Technical Standards (RTS) that DORA mandates the European Supervisory Authorities (ESAs) to produce. According to the current proposals, the majority of the RTS will be published either 6 months before or at the same time (eg, Parliament articles 16 and 18) that financial entities are expected to be in compliance. These timelines may not be possible for many financial entities. In terms of scale and complexity, the RTS in article 14 will be highly technical, including specifying cryptographic techniques. Safely making changes to cryptography could take financial entities significantly longer than 6 months. Another example is the RTS required in article 25(11), which will set out the 'detailed content' of the policy defining the use of ICT services provided by third-parties that the text requires financial entities to produce. The details of this policy could affect the operations of the financial entity, as well as the terms of its legal contracts with providers, thus requiring a period longer than 6 months to implement. The large number of RTS required by DORA and their often highly technical nature will make the RTS difficult to draft. Thus, we also do not believe it is desirable or feasible to accelerate the timelines that the ESAs have been given for their delivery. Policymakers should instead consider extending the deadline for compliance with

	DORA to 36 months from the date it enters the Official Journal of the European Union.

Proportionality

Issue/Concern	**Scope and proportionality**
Preferred text	EP text
Explanation	The scope of Oversight & Oversight Powers should be limited to services that actually attract designation and don't go beyond, as EP suggests. Co-legislators should maintain the ICT third party risk management requirements on 'critical or important functions' and ensure it is proportionate given the breadth of the definition of 'ICT services'. This will focus important obligations on arrangements that actually impact the digital resilience and stability of the financial sector. Both the Council and EP texts propose adding this clarification throughout Chapter V, Section I (see eg, article 25).

Issue/Concern	**Focus of the oversight on critical or important functions**
Preferred text	Generally EP text, Council text on article 27(2)
Explanation	The co-legislators should focus ICT risk management requirements on 'critical or important functions', as reflected in articles 7(4), 7(5), 8(2), 10(5), 11(5), and 11(6) and 12(4) of the European Parliament text. This text better embodies the principle of proportionality, particularly given the breadth of terms like 'ICT-related business functions', 'ICT assets' or 'processes' in these provisions. The inclusion of the 'critical or important functions' language will focus the requirements on more material arrangements that actually impact the digital resilience and stability of the financial sector. Moreover, there lacks a clear mechanism in the designation process under article 28 that clarifies which services are in the focus of the oversight. The industry would thus welcome seeing in the final text the additional clarifications introduced by the European Parliament's text regarding article 30(1a), and on the fact that the oversight assessment shall primarily focus on the ICT services supporting critical or important functions provided by the critical third-party provider (CTPP) to financial entities. This provision should be included and further refined in article 31(1b) in the same sense. The Council's provisions do not seem sufficient in this regard, either. By contrast, the Council's approach in article 27(2), which narrows the obligations of key contractual provisions to services concerning critical or important functions, are welcome.

ICT risk management

Issue/Concern	**Multi-vendor strategy**
Preferred text	EP text

Explanation	We strongly support the changes introduced by the European Parliament's to article 5 (9g), which focus on identifying key dependencies on ICT third-party service providers and detailing exit strategies about such key dependencies. This approach brings more clarity and legal certainty than the Commission and Council's draft texts.

Cyber threat reporting

Issue/Concern	**Significant cyber threat reporting**
Preferred text	EP text
Explanation	The trilogue parties should follow the European Parliament and adopt the voluntary regime for reporting significant cyber threats proposed by the EP (see lines and 333a, 336a and 343d). This is more appropriate than a mandatory requirement, given that cyber threats occur very frequently. Therefore, the practical impact of an obligatory reporting will be disproportionate and the obligatory incident reporting may reveal vulnerabilities that could be exploited by malicious actors. Also, we need to monitor the potential overlap between threat reporting requirements under DORA and the Revision of the Network and Information Security Directive (NIS2). A voluntary regime is also more suitable given the limited detail in DORA regarding how and when to notify cyber threats. It is clear that given the different nature of cyber threats and incidents they cannot be handled identically. Financial entities would require a clearer notification framework if notifying cyber threats were mandatory. Additionally, the European Parliament's proposal to limit cyber threat reporting to National Competent Authorities (NCAs) - who can then communicate to Financial Institutions (FIs) – is also welcome. The approach taken by the European Parliament text with respect to communication of cyber threats – ie, to share such information with relevant competent authorities (and on a voluntary basis) (see line 343d) is appropriate. Communicating cyber threats to users/clients, as contemplated in the Council text (see line 344), would not seem to be an appropriate approach. Not only is the information more confusing and alarming than helpful to these recipients, but such broad distribution of threat intelligence could lead to heightened security risk.

Incident reporting

Issue/Concern	**Incident reporting**
Preferred text	Depends on the issue
Explanation	The Council's definition of major ICT-related incidents - incidents that actually occur (as opposed to those that could occur) and have an impact (as opposed to those that could have had an impact) - is welcome. As such, the trilogue parties should adopt the Council text for article 3, first paragraph, point (7a) (line 130). This will focus obligations (eg, reporting) on incidents that actually impact users / critical functions. This is proportionate given the breadth of the definition of ICT-related

	incidents. Further, it will reduce the risk of over-reporting, which could itself inadvertently cause issues with incident response. By contrast, the European Parliament's approach to timing is appropriate and in alignment with the suggested timeframes in the horizontal legislation. Timing should be addressed in the Regulation (to avoid fragmentation, etc) and should refer to the time when the Financial Institution (FI) first became aware of an incident. The amendments made by the European Parliament to article 17(3) are welcome, specifically the European Parliament language which is more likely to ensure certainty and harmonisation by setting out the timeframe for the initial notification within the Regulation (and does not rely on a regulatory technical standard). The 24 / 72 hour frame set out in the EP draft will help ensure notifications are meaningful and actionable, and will allow financial entities to focus on response / containment in the immediate aftermath of an incident. The European Parliament's flexibility and pragmatic approach to reporting is also valuable. This recognises that not all the info is available. The amendments made by the EP to article 17(2) (see line 344) will reduce the risk of over-reporting, which could itself lead to heightened security risks. This is particularly the case for the European Parliament language requirement of informing users/clients about major ICT-related incidents only when the incident actually occurs and has material impact. Further, applying the requirement to inform users/clients if countermeasures prevent harm is also positive, as informing users/clients of risks that did not materialise (including because of effective threat management), would be confusing (and potentially alarming). Lastly, it is important that the timing of the incident reporting begins not when the financial entity becomes aware of an incident, but from the point at which the financial entity 'determines the incident to be major'. This change would reflect the reality that an incident may occur that does not immediately meet the threshold for reporting and only later, possibly even after a number of days have passed, do circumstances change such that the incident becomes a major ICT-related incident. Under the current drafting, financial entities could find themselves to be immediately in breach of the requirements.

Digital Operational Resilience Testing

Issue/Concern	**Frequency of threat-led penetration testing (TLPT)**
Preferred text	Council text
Explanation	While the Council and Parliament are largely aligned in their approaches to digital operational resilience testing, one major difference is the Parliament's inclusion of a 3-yearly minimum frequency for TLPT. The Council instead chooses to leave the frequency of testing to the national competent authority to decide. The Council's text is preferable as not all authorities have the same resources or experience with such testing and a 3-yearly cycle may be unmanageable. In our experience, even the best resourced regulators do not require supervised financial entities to undergo testing at that frequency. Connected to that is the concern that in order to comply with this requirement, NCAs may be forced to limit the number of financial entities required to take part in such testing to a smaller group than they would like or would be justified. Leaving the timing of TLPT up to NCAs does not preclude testing

	at greater frequency. However, it does allow for NCAs to consider the risk profile and number of financial entities under their supervision along with the resources they have available to dedicate to the work.

Issue/Concern	**Setting the Scope of TLPT**
Preferred text	EP text
Explanation	The Parliament's text includes an important clarification regarding the scope of TLPT in the last sentence of article 23(2). It is important for this clarification to be maintained. A large financial entity, such as those in scope of article 23, will have a significant number of critical or important functions. It is both impractical and risky to attempt to subject all such functions to a single TLPT. It is also the case that there will be a high degree of overlap between the security defences for all critical or important functions which is what a TLPT is designed to test. Parliament's text has recognised this by clarifying that it is not necessary for a single test to cover all critical or important functions. This creates a level of flexibility for the national competent authority and the financial entity to determine the precise scope of the test as required in article 23(1). This is an important consideration and therefore the Parliament's text should be preferred in this instance.

ICT third-party risk management

Issue/Concern	**Recognising the difference between intragroup and external outsourcing**
Preferred text	EP text
Explanation	Regulators around the world are reviewing requirements for third-party and technology risk management. This includes global policy setters such as the Financial Stability Board (FSB) and the International Organisation of Securities Commissions (IOSCO), which have recently published papers on outsourcing[2]. In the papers these global policy setters recognise that intragroup outsourcing creates different, although not necessarily less, risks. This is important as it implies that different risks may need to be mitigated in different ways. DORA currently considers intragroup outsourcing to be the same as external outsourcing and requires financial entities to take the same measures for both. There are important areas, such as concentration risk assessment, exit plans and termination rights, that financial entities should approach in a different way. Parliament's text has recognised this concern with amendments to articles 25(2), 27(20j) and 27(2.k.iia), which should be maintained in the final text. In addition, further amendments should be made to article 26(1. Subpara 2) to reflect the need for financial entities to tailor their solutions to the specific circumstances of intragroup outsourcing.

[2] International Organisation of Securities Commissions, "Principles on Outsourcing", October 2021, p.16 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf; Financial Stability Board, "Regulatory and Supervisory Issues Relating to Outsourcing and Third-party Relationships, Nov 2020, p.20 https://www.fsb.org/wp-content/uploads/P091120.pdf.

Oversight of ICT providers

Issue/Concern	**Allowing necessary time between designation as critical ICT TPP and the status coming into effect**
Preferred text	NA
Explanation	The changes made by the European Parliament to article 5(9g), which focus on identifying key dependencies on ICT third-party service providers and detailing exit strategies about such key dependencies, are valued. More concretely, data portability for B2B cloud users should be seen as an opportunity for cloud switching and for avoiding vendor lock-in. Accordingly, it should not be mischaracterised as a requirement for the cloud providers to migrate data, but rather be delineated as a possibility for clients/data owners to port their data between various cloud vendors' services. While the EP's approach brings more clarity and legal certainty than the Commission and Council's draft texts, the Council's stance on assessing the need for a multi-vendor strategy is appreciated. While we acknowledge the importance of avoiding concentration risk, a requirement that institutions must implement a multi-sourcing strategy can create confusion as to what that entails in practice, increase complexity in internal governance, and potentially raise risk on the financial entity. Instead, it is important to make clear that a multi-vendor strategy should remain primarily in the hands of the financial entity, based on their risk assessment and business priorities, internal governance, expertise and know-how. It is important that sufficient time is allowed between the designation of an ICT third-party as critical and that status coming into effect. This is to allow financial entities to negotiate the necessary contractual changes required to implement the requirements of DORA chapter V. It is also the case that financial entities may need to make operational changes, such as adjustments to exit plans or even to source an alternative provider if terms cannot be agreed. All of this is likely to take longer than the current six month maximum allowed by the Parliament's text. If financial entities are not allowed sufficient time, this will further reduce their negotiating leverage and may force them to accept unsatisfactory contractual terms offered by the critical ICT TPPs. The time period between designation and the status of critical coming into effect should be at least 6 months with the possibility of extension to 12 months. This will be especially important in the first iteration of the regime, as it will include the largest number of newly critical ICT TPPs and the legal teams of both financial entities and critical ICT TPPs will still be working to understand exactly what contractual language is needed to comply with the DORA requirements.

Issue/Concern	**Due Process**
Preferred text	EP text
Explanation	The steps taken by the European Parliament to introduce provisions enabling ICT third-party service providers to be more closely involved and to enhance due process overall, are very positive. They boost transparency and ensure that the oversight processes are robust, inclusive and increase overall legal certainty and quality. For instance: • Article 28(2a), with regards to the opportunity for the ICT third-party service provider to be notified before the initiation of a critical ICT third-party provider (CTPP)'s designation assessment; the notification after the

	outcome of the draft assessment as well as the opportunity to provide a reasoned statement after such assessment. • Article. 30(3, last indent), with regards to the consultation of the CTPP on the draft oversight plan. • Article 31(2), with regards to options to critical ICT third-party service provider to provide input to and/or challenge the intended recommendation by the Lead Overseer. • Article 33(1), (2b) and article 34(1a), with regards to the safeguards concerning investigations and on-site inspections, such as reviewing in a secure manner CTPP's information, and respect of rights of the CTPP's customers not subject to DORA. The Council's provisions on due process are insufficient and do not provide the appropriate level of consultation and transparency in the Regulation, but rather leave it up to the Delegated Acts to specify.

Issue/Concern	**Disclosure of recommendations by the Lead Overseer to customers (article 27[2m] and article 37[2])**
Preferred text	Combination
Explanation	The Council draft stipulates a new contractual requirement, to disclose recommendations issued by the Lead Overseer in accordance with article 31 (1d) DORA for critical ICT third-party providers to customers who are financial entities. The addition in the Council draft could establish a contractual requirement for critical ICT third-party providers to inform the financial entity of the recommendations by the lead overseer pursuant to article 31(1d) DORA. Such recommendations may concern sensitive areas of the provider's IT systems and business model. In order to implement a proportionate obligation that takes into account both the interests of the critical ICT third-party provider and of the financial entity, we deem it preferable to apply a layered approach under which the contractual requirement stipulates the obligation that: (1) by default, the critical ICT third-party provider is required to inform the customer of the Lead Overseer's view as to whether the critical ICT third-party has complied with the recommendations previously issued. This puts the financial entity in a position to easily confirm whether the critical ICT third-party provider operates in line with the assessment of the Lead Overseer under article 30(1) DORA of the Council draft. (2) if the financial entity has reason to believe that the critical ICT third-party provider does not operate in line with the recommendations, and information on the risks identified in the recommendations are required for the financial entity to demonstrate compliance to the national competent authority under article 37(2) DORA of the Council draft, the critical ICT third-party provider shall inform the financial entity of the risks identified in the recommendations. Additional considerations:

	In any case, to ensure that the recommendations reflect the actual circumstances of the provision of the services by the critical ICT third-party provider, it should be provided with the possibility to grant the Lead Overseer with any information it believes should be taken into account for the recommendations, or to challenge the recommendations, as proposed in the Parliament draft in article 31(2). The Parliament draft further establishes an obligation of the national competent authority in article 37(2) to inform customers of the risks identified in the recommendation. This provision is redundant where the critical ICT third-party service provider is already contractually required to inform the customer about such risks. A direct communication of the identified risks between the customer and critical ICT third-party service provider appears preferable, as both parties are closer to the matter at hand, and any identified risks can be more efficiently addressed and remedied by direct communication between both parties.

Co-operation with NIS competent authorities

Issue/Concern	**Co-operation between the Lead Overseer and NIS Competent authority (articles 30[3], 31[1c], 42[2] and [3a])**
Preferred text	EP text
Explanation	It is vital to mandate the coordination between DORA's Lead Overseer and the NISD2's competent authority, especially before oversight plans are finalised (article 30) and recommendations addressed (article 31), but also before conducting investigations and inspections (article 42[3a]). Unless clear coordination is established, ICT providers would be subject to both DORA and NISD2 frameworks and face parallel, potentially conflicting, regulatory provisions. While steps taken so far by the European Parliament to amend article 30 and article 31 and foster coordination at the Lead Overseer level represent a great achievement, the Council's draft does not foresee such mechanisms at the Lead Overseer level. Indeed, while article 37(2b) of the Council draft foresees that competent authorities may, on a voluntary basis, consult the NIS competent authorities, this is not sufficient as it cannot address or prevent possible inconsistencies between the recommendations of the Lead Oversight Body and the decisions of the NIS competent authorities. For DORA and NIS 2 to co-exist successfully, such coordination should happen systematically at the level of the lead overseeing body and be compulsory.

Fines

Issue/Concern	**Fines (articles 31[4], [6])**
Preferred text	EP text
Explanation	The Council draft allows for substantial fines and establishes an obligation (eg, 'shall') of the regulator to impose penalties by default in case of a violation by the critical ICT third-party service provider. • In article 31(4) the Parliament draft grants double the period (60 instead of 30 days) after being subjected by a measure of the Lead Overseer until a penalty payment may be imposed. Additionally, the EP draft leaves the decision whether a penalty should be imposed or not to the Lead Overseer ('may decide…to impose') and explicitly clarifies that such penalty should be a last resort only, whereas the Council draft now requires the Lead

	Overseer by default to impose a penalty ('shall…impose'). In light of the principle of proportionality it would be preferable to leave it to the discretion of the Lead Overseer whether or not to impose a fine in accordance with the Parliament draft ('may decide…to impose'). • In article 31(6) the Parliament draft stipulates a range of fines of up to 1% of the average daily worldwide turnover and limits the turnover to be taken into account to that related to services provided to financial entities covered by DORA. The Council draft instead requires penalties of 1% of the daily worldwide turnover, no matter how that turnover was realised. This would oblige the Lead Overseer to always impose the same amount of penalties, no matter the type of underlying 'infringement', which would not be in accordance with the principle of proportionality and it would not leave the Lead Overseer the necessary discretion to take into account the specificities of each case. • We also support both the European Parliament and European Council in their alignment with the EBA guidelines and suggestion that the termination and suspension measures foreseen in article 25(8) should be preceded by other, less stringent measures. Financial entities shall be required to evaluate the possibility of termination in case of contractual breaches, but should not be required to automatically do so, especially when there is a prospect for remedy. An obligation to terminate and suspend a contract before attempting to correct existing issues, can create the material operational resilience risk that DORA is designed to mitigate.