AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Digital Operational 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 2019, 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

Executive Summary

The European Commission has tabled its proposal for a Digital Operational Resilience Act (DORA). This Act represents a good step towards a harmonised EU framework for digital resilience in financial operations. The present paper identifies certain areas within the European Commission's DORA proposal where AmCham EU believes the proposal could be further refined.

As the voice of American businesses invested in Europe, AmCham EU emphasises the transatlantic dimension and the need for a coordinated international approach to ICT risk management in this paper. The recommendations contained within this paper therefore focus on building on existing international practices and call for openness to incorporating international best practices into the implementation of the EU's digital operational resilience.

The issues addressed in this paper include general principles; cloud computing; third-country provisions; intragroup delegation; ICT risk management; legislative consistency; the designation critical third-party providers; testing; incident reporting; EU oversight of critical third-party providers; contractual arrangements; outsourcing and sub-outsourcing; cyber threat information sharing; sanctions and penalties; oversight fees; and the implementation period.

Introduction

We recognise that an increasing digital financial services sector raises the importance of ICT and security resilience for firms. We believe the European Commission's proposal is a positive step towards a harmonised EU framework and designed to improve the digital operational resilience of financial services firms across the EU. However, we believe there are certain areas of the proposal which may need to be adjusted or clarified to best achieve the desired objectives. If such a far-reaching regulation is to be introduced in its current form, ample time should be given to all stakeholders to comply with its requirements, as well as for policymakers to assess its cost implications and consequences on innovation in the digitalisation of finance. The care we need to adopt in considering this new proposed regulation is additional compared to any other new measures, due to the peculiarities of the sector, its fast evolution, the diversification of the offering of clouds and, in future, potential development of sectoral initiatives, beyond banking.

General Principles

- **The use of technology in financial services is not new:** In fact, the financial services industry has always been at the forefront of testing and adopting new technologies to transform the financial services industry, increase competition and efficiency, as well as offering new solutions to its customers. What is new is the speed of innovation covering all aspects of the financial services sector and leading to the development of new business models, services and products. The current health pandemic is further accelerating the digitalisation process, underscoring the importance of both technological innovations but also resilience to an ever-expanding number of citizens.
- **Non-discrimination:** Technological innovation is not tied to individual jurisdictions. Similarly, financial, as well as ICT services, are by their very nature international. AmCham EU is a strong proponent of technological neutrality and is therefore critical of attempts to favour one technological solution or one financial institution or technology company over another. We watch with concern any calls for data localisation, protectionism, unjustified state intervention or calls for economic sovereignty anywhere in the world. Therefore, both international and local actors would greatly benefit from principles of fair competition and non-discrimination when establishing new measures and regimes, as well as from an

increased focus on interoperability with operational resilience requirements being developed in other jurisdictions, taking into account developments by international standard setters.

- **Regulation should not hinder innovation:** The development of many technologies is still in its infancy. It is therefore important that any policy response does not implicitly limit or contain the ability of the financial services sector to test and develop new applications. Not least COVID-19 and the events of recent months have shown how digital services are one of the drivers to foster the economic recovery and to bridge the gaps that exist across Europe and with other regions in the world. Therefore, rules that unintentionally limit firms' ability to adopt technological solutions that can either support or replace legacy systems are a barrier to improving the EU financial sector's resilience. As an example, by limiting firms' ability to adopt Cloud capabilities, firms will need to continue to rely only on legacy systems and old assets, which denies them of the opportunity for digital transformation through migration to the cloud and the associated benefits in increasing agility while maintaining operational resilience.
- **The importance of focusing on critical or important functions in the ICT third-party regime:** While the 2019 European Banking Authority (EBA) Outsourcing Guidelines focused strongly on critical or important functions, DORA has expanded the scope of financial services regulation from a focus on outsourcing to all ICT third-party providers (ICT TPPs). The focus on wider ICT TPPs is aligned with global trends and appropriate, however, when combined with a shift from critical or important functions, it can create a significant compliance burden for firms subject to DORA. It also brings into scope a number of non-critical third-party relationships that will now become more complex without the operators benefitting from improved ICT risk management of financial entities. This is especially the case for smaller financial entities like FinTech start-ups who may rely more heavily on service providers by ICT TPPs. To improve the proportionality of DORA the text should be amended to include a greater focus on critical or important functions throughout, but especially in Chapter V.
- **Supervisory capabilities:** AmCham EU supports the strengthening of the European Supervisory Authorities' (ESAs) powers in the area of digital finance. ESA's will need to work very closely together and delegate the lead to avoid duplication. This would help centralise cyber competences and avoid regulatory overlaps or inconsistencies with other legislation that aims to enhance resilience of critical sector. The emergence of new technologies will also require EU supervisors to scale up their capabilities and understanding of new technologies, which could be achieved via a stronger coordination with cyber authorities like ENISA or other cyber international bodies, and by strengthening their cross-sectoral and cross-disciplinary cooperation with data privacy and cyber security supervisors, as well as relevant law enforcement agencies. AmCham EU would encourage the appointment of a single ESA as Lead Overseer for all critical third-party service providers (CTPPs), rather than allocating this responsibility to any of the three ESAs depending on the underlying use case. This would help to centralise cyber competences and to reduce competition over scarce resources. Such an approach would ensure that the supervisory process keeps pace with developments and does not inadvertently become a barrier to financial services innovation. It would also prevent regulatory overlaps or inconsistencies with other legislation that aims to enhance resilience of critical sectors. In the current text, DORA does not seem to provide an adequate mechanism to such cooperation. AmCham EU therefore recommends the development of overarching governance principles for future supervisory cooperation, especially for the supervision of ICT providers that are already subject to privacy and cybersecurity supervisory authorities. Under this, openness and transparency will be key, namely including open consultation, not just with ESAs, but also with other key stakeholders, such as the EU Commission, the ECB, and NCAs. Establishing formal relationships with the ESAs would be a major step and AmCham EU would welcome the opportunity to engage at an early stage to set up this framework.
- **Regulatory consistency:** The DORA proposal will sit within the broader EU regulatory framework relating to both banking (like PSD2), ICT (like NISD) or both (ESA cloud and outsourcing guidance). Particularly, whilst the DORA proposal foresees a clear hierarchy between DORA and NISD for financial entities, it does not do the same for the CTPPs. This creates uncertainty which has increased with the publication of the NISD2 proposal. Generally, it is crucial to ensure that the DORA proposal builds on

already existing frameworks and requirements and foresees methods to remain aligned with them without introducing unnecessary regulatory duplication, complexity or legal uncertainty.

- **Consistency in ICT definitions:** The current ICT definitions under DORA appear somewhat confusing and lacking consistency. For example, we do not think it is the Commission's intention that credit institutions or other financial entities regulated under existing EU financial services law are intended to be defined as ICT providers in DORA (even if much of the DORA regime will rightly apply to credit institutions). Nor do we believe intragroup activities within credit institutions are intended to be dealt with in the same way as services provided on a commercial basis by external third-party providers. We believe clarity regarding the precise intentions can be enhanced by improving the definitions in article 3 (15-18).

Cloud Computing

The proposal encourages the creation of a cloud computing infrastructure that is suitable for finance institutions' usage. Cloud computing delivery mechanisms such as Infrastructure, Platform and Software as a Service have been developed to provide cloud services to a diverse range of industries with different risk appetites and levels and are typically not fine-tuned to the financial services sector. There is thus tension between cost reduction through scale and less complexity with finance sector security requirements which lead to higher costs because of provisioning requirements and potential added complexity. The risk is that the market is foreclosed to only large providers which have the resources to deal with higher cost of entry requirements created by DORA's generated investment costs on security, structure, reporting and compliance to provide services to the EU financial industry. This is an understandable trade-off for more secure and resilient digital operations but it may have unintended consequences for the competitiveness of the EU financial industry and for the ability to innovate or grow FinTech in Europe.

AmCham EU believes a structured dialogue between financial supervisors, cloud service providers and financial institutions can contribute to a better understanding of the fact that having data in the cloud can be as secure (and in many cases more secure) as housing data in the organisations' own servers. Furthermore, cloud services can improve the resilience and stability of the financial system because cloud services are flexible and dynamic and benefit from security and resilience capabilities at scale.

Third-country provisions, data localisation and international dimension

Limiting the provision of services to particular jurisdictions could in turn negatively impact the cost of the service provisioning and carry cybersecurity and resilience risks. Hence, AmCham EU asks for more clarity with regards to provisions that may limit the use of third-party providers and subcontractors based outside the EU, if they are deemed critical inside the EU. While the intention of such a provision may be to reduce risks posed to the system through lack of supervisory oversight, it may actually increase risk across the system by reducing access to advanced technology and services that support firms' resilience. It may also create operational complexity and uncertainty for financial entities who wish to enter into certain supplier arrangements, but are uncertain as to whether this is allowed eg under Article 28 (9). Therefore, the principles of fair competition and non-discrimination must be applied in the design, adoption and implementation of the new measures. In addition, the lack of clarity under Article 28 (9) could lead to additional data localisation requirements as opposed by GDPR. AmCham EU recommends GDPR-based solutions to allow for jurisdiction over non-EU providers, as well as to ensure the free flow of data which is key in Europe's role as an open, innovative and competitive digital market. Moreover, limiting the provision of services to particular jurisdictions can negatively impact the cost of

the service provisioning and carry cybersecurity and resilience risks. We also caution that Article 28 (9) is impossible for financial services firms to enact in practice as they would not be able to gain access to the information necessary to assess the criteria in Article 28 (2). This could therefore result in a de-facto ban on non-EU ICT third-parties putting EU financial entities at a significant competitive and resilience disadvantage and inviting retaliatory measures from other jurisdictions.

AmCham EU seeks clarity on the following aspects:

- **The use of third-country ICT service providers**. Article 28 (9) states that 'financial entities shall not make use of an ICT third-party service provider established in a third country that would be designated as critical'. Alongside the lack of clarity as to the designation criteria, it raises concerns that financial entities might have to make their own judgement on which of their third-party providers they expect to be critical and make decisions on their future contracts accordingly. Financial entities might not have the resources, competences or expertise to make such a judgment. This assessment should instead fall under the regulators' competence and responsibility. This uncertainty to determine which ICT providers can be deemed CTPP will be all the more problematic because of the delaying impact of Article 28 (4). Predictability of outcome and timing are key to ensure financial services companies are awarded the necessary certainty and time to adapt and ensure alignment and compliance with the oversight framework. Some of these provisions would benefit from a calibration and fine tuning, taking into account the fact that cloud providers serve not just the financial services but also a wide range of other clients (outside the scope of the oversight by the ESAs).
- **Possibility for Lead Overseer to impose restrictions on third-party sub-contractors established in a third country for critical functions** contained in article 31 (1) d iv. While we understand and agree that reviewing and gauging the financial stability risks posed by subcontracting arrangements are in the remit of the Lead Overseer under DORA, financial entities (as well as critical and non-critical ICT third-party service providers) will have to assess the extent of relevant arrangements that could fall within the cumulative criteria, in accordance with Article 26 (2). This would also require proper assessment of structural or documentary mitigants that might be available to temper the regulatory impact of such a prohibition or, alternatively, any enhanced monitoring and reporting obligation that might be put in place. More broadly, DORA, whilst granting broad powers to the overseer to mandate changes to providers' sub-contracting practices, it does not set clear criteria as to the standards that these sub-contractors should adhere to. AmCham EU calls for further clarification, as well as proportionate requirements as to sub-contracting relationships. These proportionate conditions should also be reflected in Article 31 (1) d) iv) to create clarity for all market players under which conditions further subcontracting to non-EU countries is not allowed and avoid abrupt business impact.
- **Supervisory practice within Europe that has the effect of requiring the duplication of processes, systems and data increases operational risk and fragments the Single Market.** Investment is continuously being made to ensure regulatory expectations are met, including for local governance and oversight of service provision between affiliates. Inter-affiliate services are a vital part of the operating model of a global firm. AmCham EU members utilise global service centres to efficiently serve the needs of global clients, providing specialised expertise and the ability to implement a strong oversight and control environment. We strongly believe that this centralised approach provides better capabilities and protection for a financial institution as a whole, for our local operations, and for the global financial system.
- **The proposal introduces new definitions for certain terms that are inconsistent with internationally recognised definitions as part of the Financial Stability Board's (FSB) Cyber lexicon**. To avoid any regulatory uncertainty, these definitions should be amended to be consistent with the FSB Cyber Lexicon definitions where possible.

Clarity regarding intragroup delegation, including to third country entities

The vast majority of AmCham EU's financial services members have legal entities in the EU to which the DORA regime will naturally directly apply. Moreover, the existing supervisory requirements ensure that the appropriate national and EU authorities have legal oversight and established interlocutors within the EU for complying with the obligations under DORA. However, there is currently a lack of clarity regarding the extent to which firms with third-country headquarters can delegate or outsource actual tasks required under the regulation to other entities within their group outside the EU. If EU-based entities covered by the regulation are prevented from such delegation or outsourcing, there is a risk that they may not be able to delegate or outsource certain tasks. This may result in a requirement for significant operational changes to how firms undertake digital operational resilience, without providing any additional resilience benefits.

ICT risk management (governance, framework, systems, identification, protection, detection, response, recovery)

AmCham EU supports the approach taken in DORA to allow for further technical details to be developed by the ESAs and delivered through regulatory technical standards. Yet there are levels of detail that we believe are not appropriate for either legislation or regulatory technical standards. However, a balance should be maintained between DORA's aim to achieve harmonisation on the one hand, and the desire to allow flexibility in the regulation to account for innovation and technological change on the other. However, we believe this balance has not been reached in several articles of DORA.

A focus on governance and risk management, based on capability and maturity models in proportion to a firm's risk profile, would thus be a good way to ensure that the financial sector retains the flexibility needed to adapt resilience practices to the demands of rapid technology changes and an evolving threat landscape. In particular, technologies and processes used as part of the ICT risk management framework of a financial firm should be appropriate and proportionate to the nature of the firm's operations in order to achieve the best possible outcome for security strategies.

Consistency with existing EU legislation and oversight

The interaction with other regulatory instruments like ESAs Outsourcing Guidelines and NIS Directive needs to be clarified. The approach to third-party risk management builds on the existing requirements of ESAs Outsourcing Guidelines. Whilst the DORA proposal foresees a clear hierarchy between DORA and NISD for financial entities, it does not do the same for the CTPPs. This could lead to conflicting obligations for third-party providers, especially with the new NISD2 regulatory proposal launched at the end of last year. The NISD2 draft brings many technology providers, including specifically cloud providers, under comprehensive supervision of the cybersecurity authorities with regards to ICT risk management and incident reporting. Whilst the proposal is at an early-stage, it may create a substantial overlap between the regulatory powers under NISD2 and DORA over the same cloud and infrastructure providers that will be in scope of both regulatory frameworks. It is essential for policymakers to establish a clear hierarchy between the two instruments to avoid the unnecessary duplication and fragmentation of compliance. Providers' obligations covered under the regulatory supervision of DORA should be clearly exempt from the scope of NISD2.

We would also propose to give a greater role to ENISA under DORA, eg in the processes for setting ESAs guidance on testing and incident reporting to ensure better alignment between the various regulatory frameworks, as

well as reviewing the Lead Overseer's recommendations with regards to the CTPPs security and testing practices. ESAs could also be given a mandate to exchange information on the supervisory findings with cybersecurity authorities to take those into account in their Oversight plans.

There also needs to be more clarity on the interplay with the DORA provisions and current GDPR risk management requirements, as well as with the existing ICT outsourcing guidelines. Several DORA provisions around risk management duplicate existing GDPR requirements for records of processing activity. In order to avoid imposing a disproportionate financial and administrative burden on CTPPs, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. Where we ask for more reflection is on the proportionality principle, based on some considerations including: i) scope is broader than banks; ii) tailored rules for certain categories (advanced digital testing only for significant financial entities); iii) tailored rules for certain aspects (ICT-related incident reporting only for major ICT-related incidents).

Designation of critical third-party providers

The proposal outlines that the Lead Overseer, based on recommendation of the Oversight Forum, will decide whether a TPP is considered critical. Uncertainty about the structure, members and knowledge base of the Oversight Forum, as well as to what criteria will be used, can have a significant impact due to direct oversight.

A structure as the one foreseen under the GDPR, where one national competent authority takes the lead responsibility of oversight for a respective critical third-party provider and acts as a one stop shop for all other competent authorities, would have eased the oversight and cooperation model between EU authorities. Non-EU technology companies are already familiar with such a structure, which we believe minimises the risk for introducing sectoral specificities into the framework; in this case for the financial services sector. It also allows to manage the risk of regulatory inefficiencies, overlaps, and uncertainties that we are currently facing between DORA and NISD2 in relation to ICT services. Nonetheless, we accept that the current DORA proposal introduces a new oversight model and would focus our comments on the following aspects of the proposed legislation.

On the definition of third-country ICT service provider: The DORA Regulation includes various provisions on how to manage risks posed by ICT third-party service providers. However, the proposed definition of 'ICT third-party service provider' and 'critical ICT third-party provider' do not offer sufficient clarity regarding the EU's intended scope. For example, it is not clear whether credit institutions which also provide ICT services within a group context are intended to be included in the scope of this definition or not. It would also be useful to clarify with additional language in a recital that financial entities subject to DORA are not intended to be ICT TPPs themselves, as this would result in a dramatic increase in the complexity of EU financial services regulation in the EU hurting business while not improving resilience.

On the designation process itself: The proposal states (Article 28 (1) b)) that the Joint Committee will 'appoint either EBA, ESMA or EIOPA as Lead Overseer for each critical ICT third-party service provider, depending on the total value of assets of financial entities making use of the services of that critical ICT third-party service provider and which are covered by one of the Regulations. The appointment of the lead overseer based on the customers or purely on the operations and functions for which the customers use the CTPP services may not produce the optimal choice in terms of the expertise at hand. Further, the formula outlined in article 28 (1) b) needs to be clarified. Making the appointment of the Lead Overseer depend on such a formula creates the risk that, for a given CTPP, the Lead Overseer could change over time, creating uncertainty and inefficiencies.

The framework does not clearly state the level at which the oversight will take place – ie whether it will take place at group level (the entire firm receiving oversight) or subgroup level (the specific services that the company provides that are deemed critical). This is an important distinction, as oversight conducted at group level could risk creating an uneven playing field at the sub-group level if one entity designated as critical and therefore

bearing the costs of oversight is competing with another which is not. It would be disproportionate and inefficient to grant Lead Overseers powers over all the ICT services of a given CTPP, including those which are not used by financial entities for critical and important functions or not at all, simply because one of its services is used for critical functions of financial entities. This can be addressed by narrowing the scope of Article 28 (1) a) or by reducing the scope of the Lead Overseer's powers under Article 31.

Clear criteria for designation should also be set out in the regulation (and not a delegated act). We are concerned that foreseeing additional criteria setting by delegated act (Article 28 (3)) may lead to uncertainty on the market. Having all criteria for the designation of CTPPs in the text of the DORA regulation will speed up DORA's entry into force and create clarity for both financial services entities and potential CTPPs. This is all the more relevant since there may be a period of transition and uncertainty between the adoption of the Regulation and the designation of CTPPs.

Designation criteria could be improved as follows:

- **Transparency of designation process:** The current criteria for designation of critical ICT third-party providers (Article 28) does not provide sufficient clarity to determine third-party providers designated as CTPPs. In instances where this might arise, there should also be clear processes to appeal and remove the CTPPs from designation. Providers designation as critical should be also published for transparency and comfort of the financial entities using the said providers.
- **Clearly defined scope:** The scope needs to be clearly defined and apply to the providers services used by the European financial entities for critical and important functions only – in line with the ESAs Outsourcing Guidelines approach. Otherwise, there is a significant risk of collaterally capturing less relevant services, which will negatively impact the proportionality of the regulation and inadvertently make the oversight more complex and less effective as a result.
- **Notion of criticality in relation to other regulations:** It is not straightforward for a firm to assess whether they will be considered critical based on previous European Union regulations and the current outsourcing guideline's definition of 'critical functions'.
- **Preparation Time for Compliance:** Due to the pace at which DORA is expected to move through the EU's legislative process, greater transparency from the outset regarding the designation process would be highly beneficial so that those firms which are to be designated as critical ICT third-party providers have preparation time for compliance with the regulation.

Testing, especially penetration testing

While firms today use testing, eg threat led penetration testing (TLPT) to identify risks and vulnerabilities, new techniques, such as enhanced continuous monitoring tools will, in the future, provide better real-time awareness of risks and vulnerabilities. We therefore suggest that requirements related to testing are minimised in the regulation or dealt with in regulatory technical standards.

There are risks associated with penetration-testing and TLPT, while the results of such tests are themselves a source of risk that can reveal highly sensitive data about a firm's operations. Firms must treat penetration testing results with the greatest care and confidentiality, including when sharing with regulators. It is for this reason that Article 23(2)(4) should reflect the best practice of minimising the sharing of information and the involvement of third-parties (including regulators) in the conduct of TLPT.

The text currently does not adequately allow financial entities to target testing to areas of risk. Article 21 (6) and 23 (2) should both be amended to allow for a greater focus on risk. This would be consistent with the current approach of the EBA Guidelines which require firms to perform tests 'commensurate with the risk identified' (EBA ICT and Security Risk Management Guidelines, 2019, para 43.b). This is especially important for TLPT testing in Article 23 (2). While we agree that 'critical functions and services' is the range within which a TLPT should be performed, the current text implies that all critical functions and services should be tested. Such a wide scope

would make it difficult and operationally unfeasible for the entity to control for risk. Financial entities must be allowed to scope a TLPT to a narrower set of critical functions and services.

The proposal correctly requires of penetration testers to be insured, however, the insurance premium for that risk is likely to be very high and will therefore make the cost of the whole operation cascade down the customer chain. Therefore, alternatives would need to be considered that would meet the requirements of testing security without creating disproportionate cost or risking operational systems.

When providers are required to participate in the customer testing, the nature of different cloud environments, which may include multi-tenancy, needs to be duly considered and alternative options also accounted for – to minimise inadvertent risks. Moreover, whilst we agree that cooperation between firms and their providers for testing purposes is important, it needs to take into account that cloud services may be one-to-many multi-tenant environment or may be a dedicated cloud resource. From this perspective, if a public cloud provider is deployed, the cloud vendors concerned cannot simulate a disruption of its service to support a single customer's testing because this could impact the integrity and security of the operations of other customers. At the same time, CSPs provide tools to customers to perform independent testing and simulate disruptions of their own cloud resources. If collaborative testing is required, it is critically important that such exercises remain voluntary, risk-based and bilaterally agreed upon between customers and their providers.

International financial services groups operating around the world may be subject to different digital operational resilience and testing frameworks in different jurisdictions. To avoid the risk of regulatory fragmentation and potentially costly requirements for separate tests to be undertaken in each jurisdiction, policymakers should include in the regulation a mutual recognition framework allowing TLPT tests undertaken in trusted third countries to be recognised under this framework. There are also currently no provisions allowing recognition of TLPT frameworks' test results undertaken in jurisdictions outside the EU. Alternatively, organisations should be allowed to meet their penetration testing requirements by conducting such tests with a respectable auditing firm. The produced certificates would be valid for a period of time which should be sufficient to defer repeated auditing and testing per customer or group of customers.

Incident reporting

The recently developed FSB toolkit on Cyber Incident Response and Recovery (CIRR) sets out best practice for incident reporting. It is currently unclear how the requirements in the proposal interact with those in the FSB toolkit. To avoid regulatory uncertainty, policymakers should look to ensure they are consistent.

Article 17 requires financial entities to report 'major ICT-related incidents', which are defined as ICT-related incidents with a 'potentially' high adverse impact on the network and information systems. Contrast this with current similar EBA and EIOPA requirements which require notification of events which are occurring or have occurred and/or have adverse effect. This also contrasts with notification thresholds for incidents under eg EECC, GDPR or e-Privacy Directive, which all require notification of incidents with actual impact or at the very least 'likely' impact. In light thereof, we believe that the threshold under Article 17 is too low and could create legal uncertainty with the FSE about the need to notify or lead to a situation where regulators are overwhelmed with notifications that are not helpful. Therefore, we ask EU policy makers to consider changing the threshold in DORA, by replacing the concept of 'potentially high adverse impact' so as to reflect a risk-based and proportionate angle, in order to avoid over-reporting or non-significant incidents due to the threshold being set too low.

Reporting should not be delegated to the critical service providers, or at the very least the criteria for delegation should be clarified. Moreover, delegated reporting as proposed in Article 17 (4) should be avoided, or only be allowed if/after such delegation is explicitly requested by a financial entity and an ICT provider in a particular case. Indeed, in most situations, ICT providers – who are practically offering only a part of a financial entity's ICT – will lack sufficient information to do such incident reporting or make the determination as to whether an ICT-related incident is major. More so, it would not be appropriate for ICT providers notifying ICT incidents without

the financial entity knowing. Therefore, if the delegated incident option is kept, we believe it is relevant to foresee that it requires not only approval from the national competent authority, but also an explicit request by the financial entity and the ICT provider. This would ensure clarity to the parties concerned on the conditions for a possible delegation. Generally, the basic assumption should be that accountability for reports submitted and their accuracy remains with the financial entities.

In addition, we worry that the interaction between DORA and PSD2 could lead to a more fragmented incident reporting framework. Under DORA, payment service providers (PSPs) will be excluded from ICT-related incident reporting under PSD2 but would still have to report other major operational or security incidents that are not considered ICT-related incidents under Article 96 (1) PSD2.

As mentioned above, we believe that ENISA should have a decisive role in developing the standards referred to in Article 23 (4) in addition to EBA, EIOPA and ESMA.

The proposal also facilitates incident reporting in the sense that financial institutions will only have to report 'major' ICT related incidents once to the competent authority assigned to them under Art. 41 DORA. Although the steps taken on information sharing signal a step in the right direction, the proposal needs to consider establishing a form of indemnity, under which information sharing between ICT service providers and financial institutions should fall. DORA should facilitate information sharing between ICT providers and financial institutions and provide liability protection for good faith information sharing. Further improvements need to be made in relation to cybersecurity requirements to provide a more solid legal basis for cybersecurity operations by financial institutions of by ICT service providers acting on their behalf, or for information sharing between them.

EU oversight of critical third-party providers

Many of the providers to be in scope and their financial services customers operate in a cross-border manner. Therefore, any other approach could lead to overlapping or even conflicting requirements for ICT providers and their financial services customers, as well as potentially increased operational resilience risks.

Operational resilience is part of the overall risk management framework and segmenting its supervision by allocating its responsibility to a different authority may reduce the capacity of the lead supervisory to holistically apprehend the risk exposure and mitigation efforts. Nonetheless, it is important that the ESAs contribute strongly and effectively to the convergence of supervisory practices and standards across NCAs in order to avoid the fragmentation that the new framework is meant to achieve.

Thus, AmCham EU supports the Commission proposal and believes that the core powers need to remain with the Lead Overseer. This avoids regulatory and supervisory fragmentation. From this perspective, we welcome the proposal to centralise the reporting of major ICT related incidents to conduct root cause analysis and draw lessons to foster convergence, but also identify any adaptation to the framework itself. Centralisation of reporting could streamline and reduce unnecessary burden and costs (an incident in this area may likely involve more than one jurisdiction and NCA). At this stage the regulation mandates only to conduct a feasibility study, which is an area where more ambition could be expected and encouraged. Finally, we should not forget that the risk analysis should also involve the risk of potential failure in the implementation of the oversight framework.

The NCAs should only be able to take action vis-à-vis the providers in scope in coordination with the Lead Overseer or Oversight Forum. In particular, Article 30 (4) should be clarified to better outline what are the measures that NCAs can take vis-à-vis the providers. We would encourage that 'in agreement' be clarified and expanded to 'in accordance with the Lead Overseer Plan'. In addition, the word 'concerning' adds uncertainty – the measures that the NCAs can take vis-à-vis CTPPs should be clarified. Moreover, Article 29 (4), which empowers the ESAs to issue guidelines on the cooperation between the ESAs and the NCAs, should be clarified to better outline their respective powers. To ensure regulatory consistency, it should be clear from both the provisions and recitals that the NCA is able to take decisions affecting CTPP only when acting in full accordance with the Lead Overseer's guidance and decisions.

The designation process should also seek to address the cascading effects caused by critical third-party providers themselves using other critical third-party providers.

In light of the above, the designation and oversight of critical third-party providers by the Lead Overseer should be limited to the relevant part of the providers' business: in our view it should only apply to the ICT services of the provider that are identified as critical for the EU financial entities (used for critical and important services – in line with the ESAs Outsourcing GL). Additionally, DORA should consider that CTPPs might contract with different European financial entities out of their different European subsidiaries and allow for this level of commercial flexibility.

Oversight should not create a situation of conflict of laws either for the financial entity or for the CTPP. The provision of ICT and financial services are inherently global. Both CTPPs and financial services are likely to have complex corporate structures across multiple jurisdictions (including outside the EU). There should be boundaries in the powers of the Lead Overseer to compel changes or to compel the provision of information that concern subsidiaries outside its jurisdiction, as this could create conflicts of laws with other jurisdictions.

Oversight process, recommendation and follow up

There needs to be a consultative process not just with ESAs, but also with the other key stakeholders, such as the EU Commission, the ECB, and NCAs and the designated providers before the recommendations/requests to a critical third-party provider are finalised and enacted to be able to fully understand and address the foreseen requirements.

- There needs to be a clear appeal process for providers.
- Timing for response should be reasonable and proportionate to the nature of the findings.
- Requests for information, general investigations and onsite inspections by the Lead Overseer need to respect different cloud environments such as multi-tenant, not cause disruption of services which would create risks, and provide for safe harbours for customers not in scope of the regulation as well as remove risk of liability of the providers vis-a-vis their customers.
- Termination of contracts by the NCAs (Article 37) is a last resort. It needs to follow a due process (consider a system of warnings first) and should only be done in coordination with the Lead Overseer or Oversight Forum. Moreover, termination of contracts should apply restrictively only to the contractual aspects affected by the supervisory authority findings as opposed to the contract applying to the complete commercial relationship. Often contracts are built on the basis of a multifaceted relationship therefore a finding against one aspect of that relationship should not result in a termination of the complete contract. In addition, termination does not allow for providers to address deficiencies, rather causing more disruption for financial services entities and working against the purpose of promoting ICT uptake in the sector.

The provision for the Lead Overseer to conduct on-site inspections covering 'the full range of relevant ICT systems, networks, devices, information and data either used for, or contributing to, the provision of services to financial entities', does not necessarily align with or recognise the way in which ICT companies operate today. Many firms use cloud storage to reduce costs by accessing flexible computing power that is commensurate with their business needs rather than committing massive investment to on-premise hardware and infrastructure. This again raises the point of conflict of laws and more broadly the extent to which the EU can assert jurisdictions to require information or inspection of such systems, especially when they serve a secondary functionality for EU financial institutions such as disaster recovery. Wide use should be made of third-party audits or other methods such as virtual tours to minimise the frequency of on-site inspections which may in themselves represent a vulnerability.

Given the novelty of the framework's structure and, in particular, the shared responsibility among regulatory authorities, there should be a mechanism in place to ensure dialogue between the CTPP and Oversight

Forum/Lead Overseer is always possible. Such mechanism should also make it possible to involve other regulators that may have co-competences such as critical infrastructure or privacy. Article 30.3 states that "Lead Overseer shall adopt a clear, detailed and reasoned individual Oversight plan for each critical ICT third party service provider. That plan shall be communicated each year to the critical ICT third-party service provider." We propose adding that the critical ICT third-party service provider shall be able to raise queries about the Oversight plan at the beginning of the year and throughout the year on an ad hoc basis.

Regulating the CTPPs in cybersecurity and resilience is a highly technical area that will require considerable expertise from the supervisory authorities. A mechanism that is already in place and has worked well with other EU agencies such as ENISA and Europol has been to create a permanent consultative structure involving stakeholders from the industry that would enable them to exchange information on policy, technology and the market developments. Such structures have been most recently created with the adoption of the EU Cybersecurity Act. It would be advisable to consider such a structure at the level of the ESAs to help inform policy makers of the different interactions and dependencies between digital, finance, resilience and cybersecurity and enable regular consultation.

Contractual arrangements

Any rules related to contractual relationships need to reflect the fundamental right of parties to enter into commercial contracts. Any mandatory terms, if introduced, need to be based on business realities and be equitable. There are a number of contractual asymmetries that have been introduced inside DORA that change drastically both existing business practices and the equitable relationship of the parties. For instance, DORA foresees very tight deadlines for termination in favour of the financial institutions, whereas all the notification timelines that financial institutions have towards their ICT providers are extended to considerable length of time – length that is not commercially reasonable or practical and creates significant uncertainty for the actions and investments ICT providers need to make.

The provision giving competent authorities power to require financial entities to temporarily suspend contracts with CTPPs may lead to legal uncertainty.

Financial entities have to define a holistic ICT multi-vendor strategy explaining the rationale behind the procurement mix of third-party service providers. Although we understand possible concerns about the procurement mix, we think that these concerns should not play beyond what is necessary to ensure resilience and sufficient levels of guarantees. We also consider that a multi-vendor strategy should not create disproportionate restrictions on customers and should notably continue allowing them to opt for certain services providers for specific needs, if this best meets their needs and provided the security concerns are addressed.

Outsourcing and sub-outsourcing

DORA needs to be consistent in scope with the ESAs Guidelines based on materiality/provisions of services for critical and important functions. It should also be clear how we transition from the current law to the new law, especially given financial entities and providers will already have existing contractual arrangements.

DORA captures in its scope software and separates that from cloud as a platform, infrastructure or service. Software, which by definition is on premise, is operated by the financial institution and goes beyond the scope of EBA Guidelines on outsourcing. Moreover, numerous requirements that may be meaningful in the context of DORA and outsourcing of CTPP using cloud computing make no sense if they are applied on a provider of critical software that is on premise therefore operated and effectively controlled by the financial institution.

When implementing the DORA requirements on risk management the policy objectives and additional costs to the industry should be carefully balanced. One example where the rules could be particularly onerous is the requirement to risk assess firmware upgrades creates additional reporting and risk management obligations that reach the level of hardware and are impractical in the current complex supply chain environment.

DORA introduces new powers for the regulators to assess and put forward requirements to sub-outsourcing, but those are not clearly defined. We believe more clear parameters and criteria outset is needed to avoid duplication or inconsistent requirements – in particular at the pre-planning stages.

Cyber threat information sharing

Positively, the proposal clarifies the exchange of information between financial institutions and supervisors. Notwithstanding, the requirement to notify authorities of participation in information sharing groups should be removed to ensure such participation remains voluntary. The text currently requires firms to notify competent authorities of their participation in information sharing arrangements, which would diminish the voluntary aspect of information sharing. Mandating participation in information sharing schemes could result in an increase of low-quality intelligence and distract resources from analysing higher-quality information shared on a voluntary basis.

Sanctions/penalties

We propose a recital to Article 31 (7) that clearly states that Lead Overseers shall only impose penalty payments as a last resort in the event that the ICT third-party provider fails to comply with its procedural obligations, such as facilitating inspections, despite other reasonable measures being taken. The size of the penalties should also be proportionate and limited to up to 1 % of the turnover of the providers' business in scope of the regulation (vs worldwide turnover) – i.e. the business of providing critical services to the EU financial entities. We recommend, in accordance with the approach adopted under numerous other regulations, that periodic penalty payments shall not by definition always amount to 1 % of the average daily worldwide turnover of the CTPP but rather to an amount up to 1 % of such turnover that is proportionate to the nature and gravity of the non-compliance.

Oversight fees

Under Article 38 of DORA, the ESAs may charge oversight fees to CTPPs. The amount of a fee charged will cover 'all administrative costs' of oversight and be 'proportionate' to the turnover of the CTPP. There are however no guarantees as to the level of the fees, the relevance of that level and the principle of equality. Therefore, in accordance with a similar regime foreseen in Article 16 EECC, we consider that Article 38 should provide that the oversight fees that the ESAs can charge should apply in a non-discriminatory way and cover only the administrative costs that they incur in carrying out the specific oversight tasks entrusted by DORA.

Implementation period

The implementation period foreseen in Article 56 of the proposal is unrealistic and inconsistent with other DORA provisions. Indeed, the proposal foresees one year to comply with the regulation, and, at the same time, it mandates the ESAs to develop technical standards within 1 to 3 years after its entry into force (with which entities will have to comply). For instance, Article 27 (4) provides that the ESAs 'shall develop draft regulatory technical standards to specify further the elements which a financial entity needs to determine and assess when sub-contracting critical or important functions to properly give effect to the provisions of point (a) of paragraph 2.' Therefore, we recommend that the implementation of DORA be at least 3 years or 24 months after the publication of the technical standards.

Conclusion

AmCham EU considers the DORA proposal to be of particular importance. Its members very much welcome the EU's effort to create a robust framework for ICT operational resilience. Not least COVID-19 has shown the growing importance of ICT infrastructures for the functioning of modern economies, including in particular for financial services.

The discussions on this proposal within AmCham EU have brought together members of both the Financial Services Committee and of the Digital Services Committee. We therefore believe our joint position captures the views of the entire industry; both that of the financial services providers and the newly covered third-party technology providers to the sector. We would hope our views can bring a unique and comprehensive view to DORA.

As AmCham EU, our paper also puts a particular emphasis on the transatlantic dimension and need for a coordinated international approach to ICT risk management. We urge the EU to build on existing international practices and remain open to incorporating international best practices into the implementation of DORA. At the same time, DORA or any other regional frameworks should not lead to any conflicts of law or overlapping requirements for financial services and technology companies operating globally.