AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Implementation of the Digital Operational Resilience Act

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 €3.4 trillion in 2021, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive summary

The three European Supervisory Authorities (ESAs) are currently tackling the operational aspects of the Digital Operational Resilience Act (DORA). In this context, businesses from both the financial services and digital sector have identified areas of the legislation on which clarity is particularly needed. In order to ensure legal certainty and allow industry to properly prepare for the new rules, the ESAs should aim to further clarify the following:

- Level of aggregation within a Group to which DORA would apply.
- Criteria and process around designating critical information and communications technology (ICT) third-party providers.
- Procedures that apply to incident reporting.
- Consistency with other EU legislation.

Introduction

DORA was adopted at the end of the last year with the intention to set uniform cybersecurity rules for the regulated financial services sector and its ICT service providers. Following the adoption, the ESAs (including the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority) work on successful implementation of DORA. Nonetheless, industry needs further clarity to prepare for this legislation and implement new rules.

Group structures

DORA does not provide legal certainty in a number of corporate structures where an IT service provider provides services to regulated entities outside the own group and might be designated as ICT third-party providers (CTPP). The ESAs should seek to provide clarity on the application of such scenarios at the earliest opportunity.

It would be beneficial if designation would apply at the level of the entity that provides critical services to the regulated sector – as was suggested in previous exchanges. This would mean that other legal entities in the same group, whether these are regulated entities or non-regulated entities, would not be subject to the oversight framework. Attention should be paid in particular to article 38.8 of DORA, which makes clear that the regulated entities would not fall under DORA. The same clarity does not exist for the other non-regulated entities of that group. Providing this explicit certainty as part of the RTS would give legal certainty to the application of DORA.

The below table seeks to capture the possible Group structures of entities that might be covered by DORA. In principle, there are three scenarios: (1) the Group consists wholly of non-regulated (ie non-

financial) entities; (2) the Group consists wholly of regulated (ie financial) entities and (3) the Group consists of a possible mix of non-regulated and regulated entities.

It is thus understood that Group which consists wholly of regulated entities should not be subject to a designation of any of its entities within the Group as ICT third-party providers (Scenario 2).

If the Group consists either of non-regulated, ie non-financial, entities or consists of a mix of regulated and non-regulated entities, only the relevant entity providing critical ICT services to the financial services industry should be designated as a ICT third-party provider (Scenario 1 and 3).

Group composition	Scenario 1: Consists of non-regulated entities	Scenario 2: Consists of regulated entities	Scenario 3: Consists of non-regulated and regulated entities
Possible designation of a CTPP and DORA oversight within the group	Yes, only the entity providing critical services to financial entities	No, as per DORA art. 31.8	Yes, only the non-regulated legal entity providing critical services to financial entities

Delegated act specifying further criteria for designation

DORA has introduced proportionality by striking the right balance between rule consistency, supervisory efficiency and cooperation. Such positive approach towards proportionality should also apply to the scope of the forthcoming oversight of critical ICT third-party service providers (CTPPs). This is particularly important given the breadth of the definition of ICT services, which in turn brings the need for a clear set of supplementing CTPP designation criteria under article 31.

Among other criteria, article 31.2 stipulates that CTPP designation shall be based on criteria in relation to ICT services provided by the ICT third-party service provider to financial entities and, more specifically, on the reliance of financial entities on such services in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider. However, article 31.1.(a) still foresees a designation on entity-level, which can lead to oversight over non-relevant services that happen to be also offered by the CTPP. Therefore, there is room for improving legal certainty and regulatory efficiency, eg by enhancing the focus on services offered by a CTPP that are critical to financial entities.

In the spirit of Article 33.2, the oversight function exercised by the Lead Overseer should mainly focus on the relevant part of the CTPP's business, ie ICT services provided by the critical ICT third party service provider materially supporting the critical or important functions of financial entities). Furthermore, according to Recital 76, DORA aims to promote convergence and efficiency in relation to supervisory approaches. Therefore, it would be inefficient if the Lead Overseer focuses its oversight

powers over all the services provided by a CTPP, including those which are not used by financial entities for critical and important functions, simply because one/more service(s) provided by the CTPP is/are used for a critical or important function of a financial entity. The parameters for CTPP designation should be targeted to ensure that oversight of CTPP's remains efficient for the supervisory authorities.

The refinement of CTPP designation criteria within the forthcoming Delegated Act that will supplement DORA, as provisioned by article 31.6, would be a positive development. To ensure regulatory certainty well-ahead of DORA becoming fully applicable, the ESA's should consider the following recommendations in relation to the Delegated Act:

- Build on the criterion set out in article 31.2.(a) to add clarifications that the CTPP designation shall specifically focus on the CTPP services which have the potential to effectively impact the digital resilience and stability of the financial sector in relation to 'ICT services' as defined under article 3(21) and in relation to 'critical or important function' as defined under article 3(22).
- Consider using a data-driven model based on the ICT third-party registers set out in article 28.3 in making assessments of which ICT third-party service providers should be designated as critical based on the on the nature of usage of services that the financial entities are deploying (including the materiality of the service to the business and potential impact to the financial entity, among others). However, the current range of registers, the variety of definitions and data collection methods to which financial entities are subject across the bloc, may make this impossible. Therefore, EU authorities should prioritise a harmonisation project for third-party and outsourcing registers as soon as possible.
- All material criteria for the designation of CTPPs should appear in the text of the forthcoming Delegated Act in order to create clarity for both financial entities and potential CTPPs.
- The Delegated Act should require that assessment of each criteria in article 31.2 by the European Supervisory Authorities should be documented in the designation. The goal is to avoid an overly broad oversight and anchor legal clarity: clear view of which services triggered designation in the first place and should therefore be the focus of oversight activities.

These suggestions would not only increase legal certainty, but also establish rules that are pragmatic, implementable and measurable to advance DORA's objectives. In the view of the financial services and ICT industry with US parentage and with global activities, the designation criteria should contribute to international consistency on the scope of ICT risk management and oversight.

Pragmatic incident reporting - thresholds, timelines and criteria

Reporting of timely and accurate incident information to regulatory authorities is crucial for addressing cyber risk. DORA's intention to harmonise incident reporting across the EU is beneficial. However, the EU should take a clear lead in pursuing further convergence in incident reporting

requirements globally. The Financial Stability Board has proposed global convergence in cyber incident reporting to ensure greater efficiency for globally active financial institutions and to facilitate easier exchange of information at critical points between regulatory authorities. Thus, the EU should seek to align with the Financial Stability Board's proposals where possible. In creating an incident reporting regime, there remains a risk that low thresholds, multiple competing criteria and unreasonable timelines could cause an inaccurate, distracting and overly cumbersome reporting regime. Therefore the EU should follow the below principles:

- **Reporting timelines**: When facing a cyber incident, a financial institution's priority is understanding how an incident could be disrupting their services or affecting their customers. Understanding the geographic reach or the economic impact is therefore of secondary importance at the stage of initial notification to authorities. Reporting timelines should focus limited resources on incident management and, at a minimum, allow firms to report no later than 24 hours post a financial institutions awareness that a major ICT-related incident has arisen. This timeline would be consistent with the Network and Information Security 2 (NIS2) Directive and the General Data Protection Regulation (GDPR).

- **Cyber incident criteria**: The accuracy of reporting information provided to regulatory authorities is crucial for an effective reporting regime. A short timeline for initial reporting alongside multiple competing incident criteria will result in information that will be inaccurate and will likely change as a financial institution's knowledge of the incident develops. As DORA requires initial, intermediate and final reporting, the ESAs should prioritise criteria e) to ensure that the authorities receive major incident reporting-only. Criteria b) and d) should be supporting criteria for further determining whether an ICT-related incident is significant. The reporting regime should not impede a financial institution's primary priority to restore their ICT services and support their customers. In that regard, while understanding that customer impact is vital, the focus in the early stages of incident management should not be on determining the exact number of customers impacted or the exact amount of transactions affected.

- **Cyber incident thresholds**: Low thresholds for incidents, in conjunction with numerous criteria, will result in an overwhelming number of incidents being reported by financial institutions. This will serve limited use to addressing systemic cyber risk by regulatory authorities and will practically cause the incident regime to be unworkable. The incident thresholds should reflect the scale of DORA in applying to all sectors within financial services and focus on reporting major incidents-only.

- **Alignment between DORA and NIS2**: DORA will establish cybersecurity requirements specifically for the financial services institutions and their service providers. These organisations may also be covered by the NIS 2 Directive, which is clearly linked to DORA. Thus, it is of utmost importance to ensure consistency and avoid unnecessary redundancy between DORA and NIS2. Harmonisation among cybersecurity laws is a well-recognised principle by EU institutions and

among regulated entities and is instrumental to promoting strong cybersecurity by simplifying compliance obligations and minimising complexity. This relates in particular to the following:

- Adoption of a 24-72-hour incident notification period consistent with NIS2;
- minimum time limits for notification for any sub-sector should be consistent with NIS2; and
- the incident report content/template under DORA should be consistent with NIS2 and the FSB's incident reporting framework where possible.

Consistency with existing EU regulation and guidelines

One of DORA's stated objectives is to harmonise European provisions tackling digital operational resilience and ICT security. Disparities and uneven national regulatory and supervisory approaches can restrict the functioning of the internal market and cause difficulties for financial institutions who operate on a cross-border basis.

The significant harmonisation already achieved by DORA is a positive step but the regulatory technical standards (RTS) should continue to pursue harmonisation where possible. As part of this important harmonisation, ESAs should align their existing guidance, which has established itself as the central framework for today's use of third-party providers in the financial sector, in accordance with DORA. During this alignment, we should continue using the existing financial services guidance that has been proven to be effective. The below constitutes an overview of other relevant regulation and guidance:

DORA provision	Other relevant regulation and guidance
ICT security policies	EBA guidelines on outsourcing EBA guidelines on ICT and security risk management
Access management	EBA guidelines on outsourcing EBA guidelines on ICT and security risk management
Business continuity	EBA guidelines on outsourcing EBA guidelines on ICT and security risk management Basel operational resilience principles
Sub-outsourcing	EBA guidelines on outsourcing
Response and recovery plans	EBA guidelines on ICT and security risk management

Political risk	EBA guidelines on outsourcing
Registers of information	EBA guidelines on outsourcing
Incident reporting	ECB major cyber incident reporting PSD2 major incident reporting GDPR FSB cyber incident reporting

Conclusion

DORA is crucial to ensure digital operational resilience and ICT security in the financial sector. However, for industry to successfully implement the new rules, several concerns should be addressed. In particular, businesses need further clarity on the level of aggregation within a Group, the criteria for designation of CTPPs, incident reporting and the consistency with other EU legislation. AmCham EU looks forward to continue cooperating with the ESAs and the European Commission to contribute to DORA's success.